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*

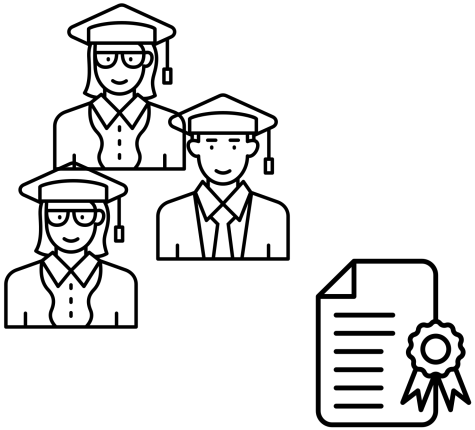
Setting: Protocol Analysis

Major Goal

Proving protocols secure

Discovering Attacks on Protocols

Classic Approach



Manual cryptographic proofs

Our Research Area

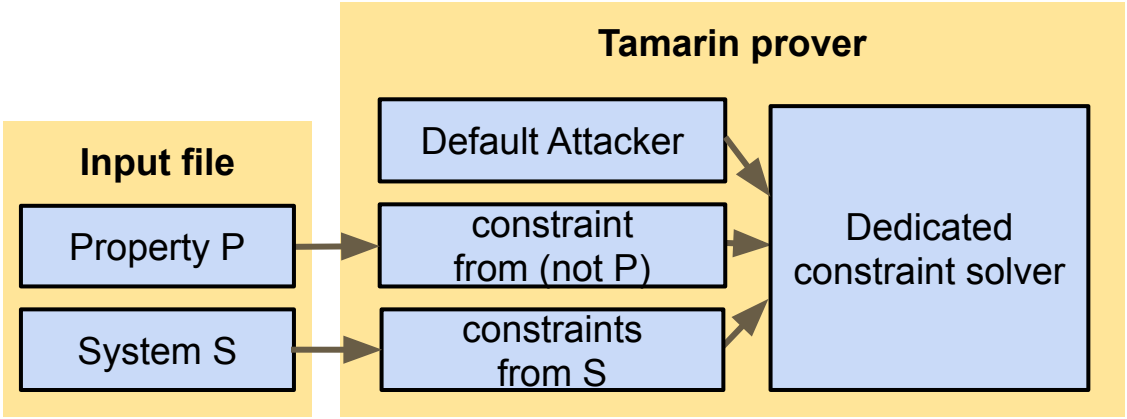
Automated Analysis

- Started in the 90s
- Big technical progress in recent years
- Used for large scale protocol analysis, e.g., TLS1.3, WPA2, EMV, LAKE.

We use the Tamarin Prover!

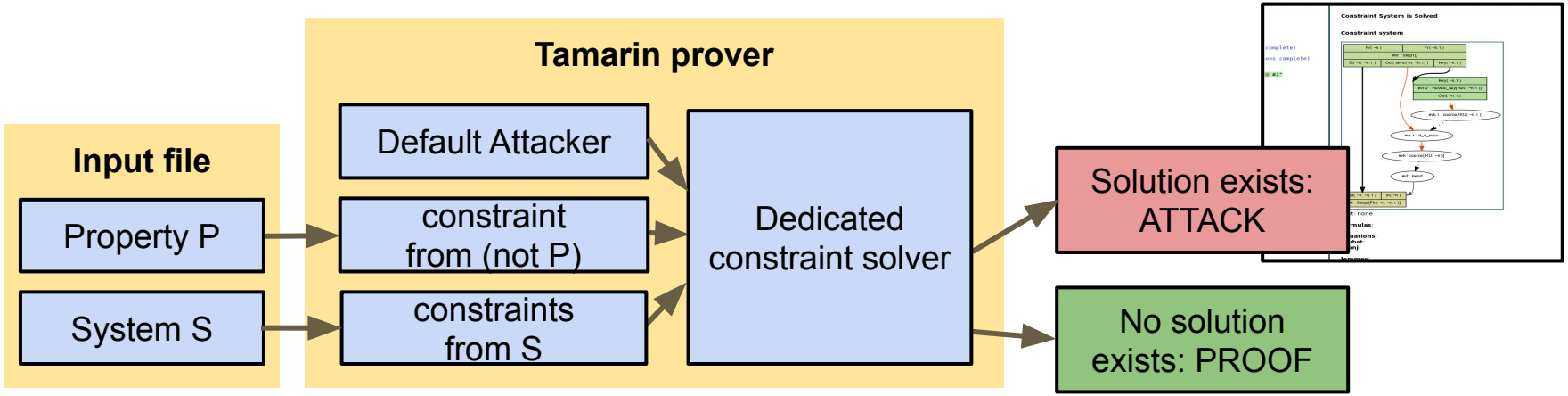
The Tamarin Prover

The Tamarin Prover



The Tamarin Prover

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY



The Tamarin Prover

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Input file

Property P

System S

Tamarin prover

Default Attacker

constraint from (not P)

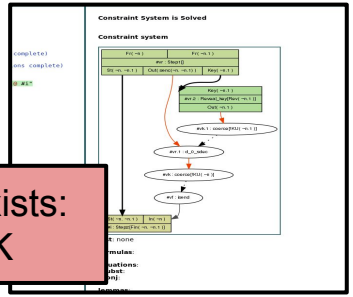
constraints from S

Dedicated constraint solver

Solution exists: ATTACK

No solution exists: PROOF

Run out of time or memory



The Tamarin Prover

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Input file

Property P

System S

Tamarin prover

Default Attacker

constraint from (not P)

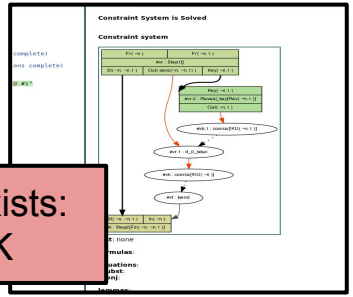
constraints from S

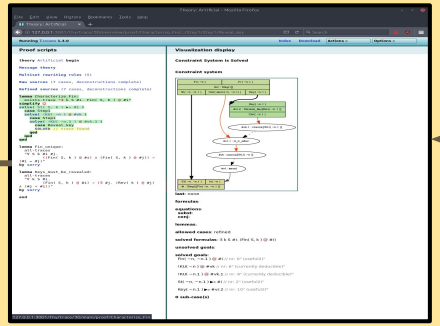
Dedicated constraint solver

Solution exists: ATTACK

No solution exists: PROOF

Run out of time or memory

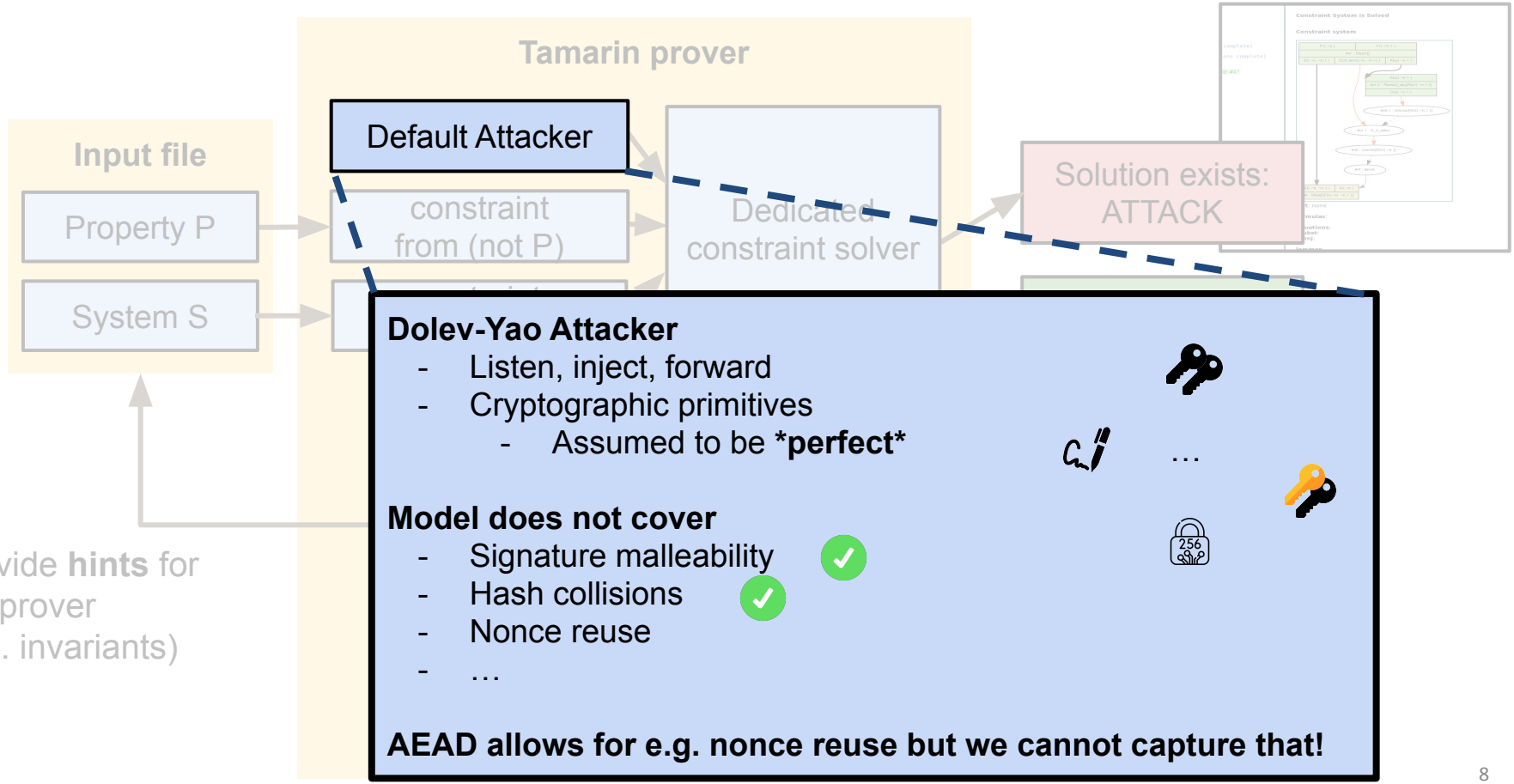




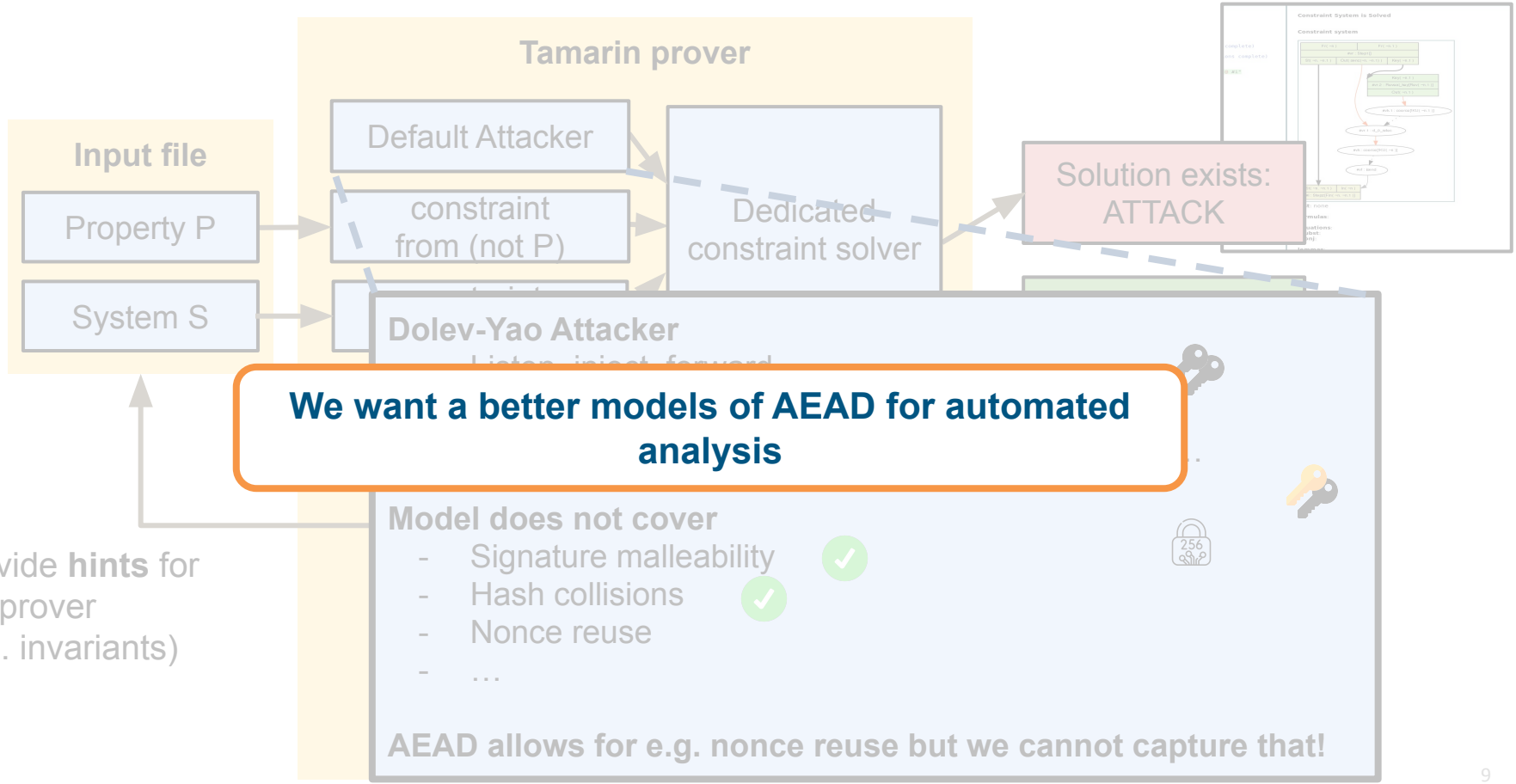
Interactive mode
(Inspect or guide partial proof)

Provide **hints** for the prover (e.g. invariants)

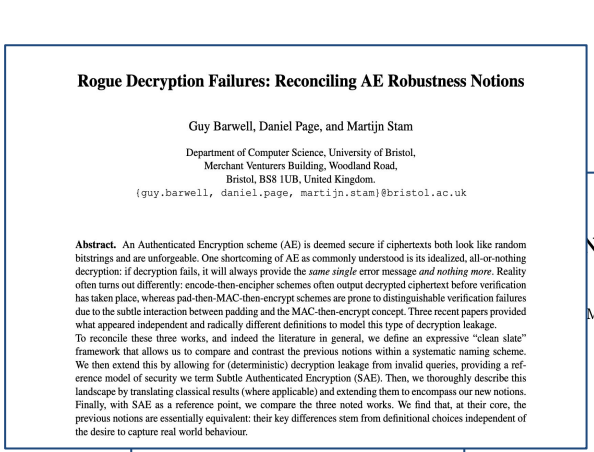
Authenticated Encryption with Associated Data



Authenticated Encryption with Associated Data



AEAD is complex!


Rogue Decryption Failures: Reconciling AE Robustness Notions

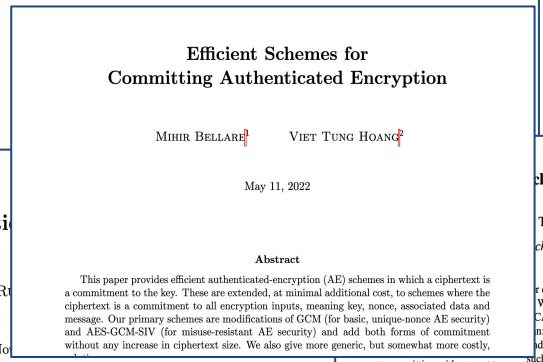
Guy Barwell, Daniel Page, and Martijn Stam

Department of Computer Science, University of Bristol,
Merchant Venturers Building, Woodland Road,
Bristol, BS8 1UB, United Kingdom.
{guy.barwell, daniel.page, martijn.stam}@bristol.ac.uk

Abstract. An Authenticated Encryption scheme (AE) is deemed secure if ciphertexts both look like random 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 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" 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 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 the desire to capture real world behaviour.


John Chan and Phillip Rogaway

Keywords: anonymous encryption · authenticated encryption · nonces · privacy · provable security · symmetric encryption

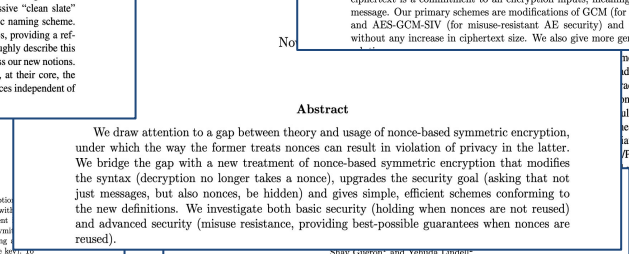

Efficient Schemes for
Committing Authenticated Encryption

Mihir Bellare[1] Viet Tung Hoang[2]

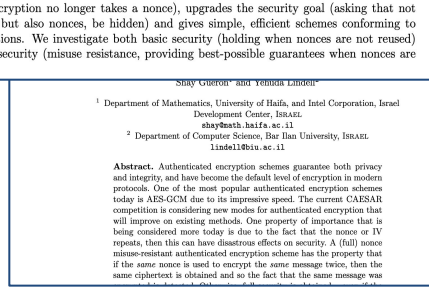
May 11, 2022

Abstract

This paper provides efficient authenticated-encryption (AE) schemes in which a ciphertext is a commitment to the key. These are extended, at minimal additional cost, to schemes where the 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) and AES-GCM-SIV (for misuse-resistant AE security) and add both forms of commitment without any increase in ciphertext size. We also give more generic, but somewhat more costly,

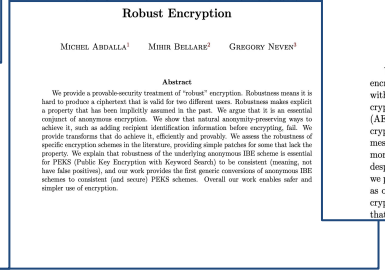

Abstract

We draw attention to a gap between theory and usage of nonce-based symmetric encryption, under which the way the former treats nonces can result in violation of privacy in the latter. We bridge the gap with a new treatment of nonce-based symmetric encryption that modifies the syntax (decryption no longer takes a nonce), upgrades the security goal (asking that not just messages, but also nonces, be hidden) and gives simple, efficient schemes conforming to the new definitions. We investigate both basic security (holding when nonces are not reused) and advanced security (misuse resistance, providing best-possible guarantees when nonces are reused).


Shay Gueron[1] and Yehuda Lindell[2]

[1] Department of Mathematics, University of Haifa, and Intel Corporation, Israel Development Center, Israel
shay@math.haifa.ac.il
[2] Department of Computer Science, Bar Ilan University, Israel
lindell@biu.ac.il

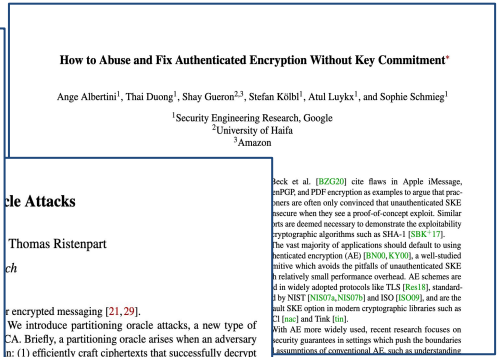
Abstract. Authenticated encryption schemes guarantee both privacy and integrity, and have become the default level of encryption in modern protocols. One of the most popular authenticated encryption schemes today is AES-GCM due to its impressive speed. The current CAESAR competition is considering new modes for authenticated encryption that will improve on existing methods. One property of importance that is being considered more today is due to the fact that the nonce or IV repeats, then this can have disastrous effects on security. A (full) nonce misuse-resistant authenticated encryption scheme has the property that if the *same* nonce is used to encrypt the *same* message twice, then the same ciphertext is obtained and so the fact that the same message was


Robust Encryption

Michel Abdalla[1] Mihir Bellare[2] Gregory Neven[3]

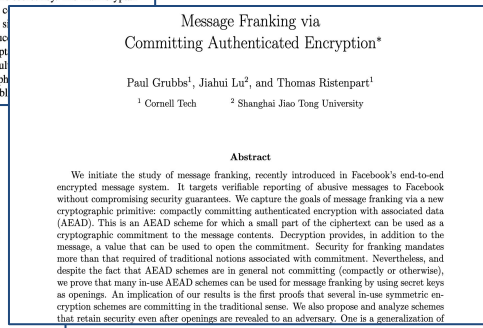
Abstract

We provide a provable-security treatment of "robust" encryption. Robustness means it is hard to produce a ciphertext that is valid for two different users. Robustness makes explicit a property that has been implicitly assumed in the past. We argue that it is an essential conjunct of anonymous encryption. We show that natural anonymity-preserving ways to achieve it, such as adding recipient identification information before encrypting, fail. We provide transforms that do achieve it, efficiently and provably. We assess the robustness of specific encryption schemes in the literature, providing simple patches for some that lack the property. We explain that robustness of the underlying anonymous IBE scheme is essential for PEKS (Public Key Encryption with Keyword Search) to be consistent (meaning, not have false positives), and our work provides the first generic conversions of anonymous IBE schemes to consistent [and secure] PEKS schemes. Overall our work enables safer and simpler use of encryption.


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
[2]University of Haifa
[3]Amazon


Message Franking via
Committing Authenticated Encryption*

Paul Grubbs[1], Jiahui Lu[2], and Thomas Ristenpart[1]

[1] Cornell Tech [2] Shanghai Jiao Tong University

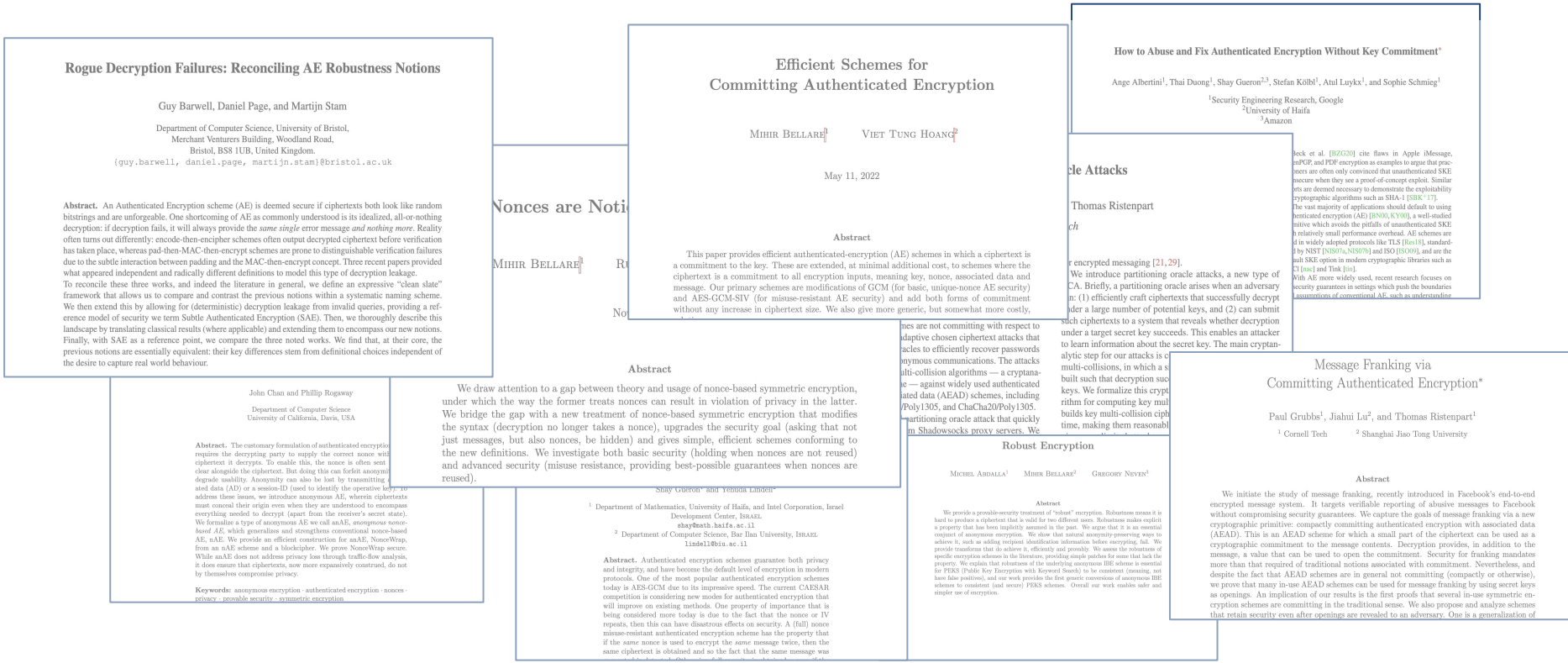
Abstract

We initiate the study of message franking, recently introduced in Facebook's end-to-end encrypted message system. It targets verifiable reporting of abusive messages to Facebook without compromising security guarantees. We capture the goals of message franking via a new cryptographic primitive: compactly committing authenticated encryption with associated data (AEAD). This is an AEAD scheme for which a small part of the ciphertext can be used as a cryptographic commitment to the message contents. Decryption provides, in addition to the message, a value that can be used to open the commitment. Security for franking mandates more than that required of traditional notions associated with commitment. Nevertheless, and 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

Only Academic Definitions!

Many competing definitions as we speak!

AEAD is complex!



Rogue Decryption Failures: Reconciling AE Robustness Notions

Guy Barwell, Daniel Page, and Martijn Stam

Department of Computer Science, University of Bristol,
Merchant Venturers Building, Woodland Road,
Bristol, BS8 1UB, United Kingdom.
{guy.barwell, daniel.page, martijn.stam}@bristol.ac.uk

Abstract. An Authenticated Encryption scheme (AE) is deemed secure if ciphertexts both look like random 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 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" 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 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 the desire to capture real world behaviour.

Efficient Schemes for
Committing Authenticated Encryption

Mihir Bellare[1] Viet Tung Hoang[2]

May 11, 2022

Abstract

This paper provides efficient authenticated-encryption (AE) schemes in which a ciphertext is a commitment to the key. These are extended, at minimal additional cost, to schemes where the 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) and AES-GCM-SIV (for misuse-resistant AE security) and add both forms of commitment without any increase in ciphertext size. We also give more generic, but somewhat more costly,

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
[2]University of Haifa
[3]Amazon

Nonces are Noti

Mihir Bellare[1] Ru

No

Abstract

We draw attention to a gap between theory and usage of nonce-based symmetric encryption, under which the way the former treats nonces can result in violation of privacy in the latter. We bridge the gap with a new treatment of nonce-based symmetric encryption that modifies the syntax (decryption no longer takes a nonce), upgrades the security goal (asking that not just messages, but also nonces, be hidden) and gives simple, efficient schemes conforming to the new definitions. We investigate both basic security (holding when nonces are not reused) and advanced security (misuse resistance, providing best-possible guarantees when nonces are reused).

cle Attacks

Thomas Ristenpart

ch

g encrypted messaging [21, 29].
We introduce partitioning oracle attacks, a new type of
CA. Briefly, a partitioning oracle arises when an adversary
n: (1) efficiently craft ciphertexts that successfully decrypt
nder a large number of potential keys, and (2) can submit
uch ciphertexts to a system that reveals whether decryption
under a target secret key succeeds. This enables an attacker
to learn information about the secret key. The main cryptan-
alytic step for our attacks is c
multi-collisions, in which a s
built such that decryption suc
keys. We formalize this crypt
rithm for computing key mul
builds key multi-collision ciph
time, making them reasonabl
m Shadowsocks proxy servers. We

Beck et al. [BZG20] cite flaws in Apple iMessage,
enPGP, and PDF encryption as examples to argue that prac-
tioners are often only convinced that unauthenticated SKE
secure when they see a proof-of-concept exploit. Similar
rts are deemed necessary to demonstrate the exploitability
ryptographic algorithms such as SHA-1 [SBK+17].
The vast majority of applications should default to using
henticated encryption (AE) [BN00, KY00], a well-studied
mitive which avoids the pitfalls of unauthenticated SKE
h relatively small performance overhead. AE schemes are
d in widely adopted protocols like TLS [Res18], standard-
d by NIST [NIS07a, NIS07b] and ISO [ISO09], and are the
ault SKE option in modern cryptographic libraries such as
CI [Inac] and Tink [tin].
With AE more widely used, recent research focuses on
security guarantees in settings which push the boundaries
assumptions of conventional AE, such as understanding

John Chan and Phillip Rogaway

Department of Computer Science
University of California, Davis, USA

Abstract. The customary formulation of authenticated encryptio
requires the decrypting party to supply the correct nonce wit
ciphertext it decrypts. To enable this, the nonce is often sent
clear alongside the ciphertext. But doing this can forfeit anonymi
degrade usability. Anonymity can also be lost by transmitting
ated data (AD) or a session-ID (used to identify the operative key). To
address these issues, we introduce anonymous AE, wherein ciphertexts
must conceal their origin even when they are understood to encompass
everything needed to decrypt (apart from the receiver's secret state).
We formalize a type of anonymous AE we call anAE, *anonymous nonce-based AE*, which generalizes and strengthens conventional nonce-based AE, nAE. We provide an efficient construction for anAE, NonceWrap, from an nAE scheme and a blockcipher. We prove NonceWrap secure. While anAE does not address privacy loss through traffic-flow analysis, it does ensure that ciphertexts, now more expansively construed, do not by themselves compromise privacy.

Keywords: anonymous encryption · authenticated encryption · nonces · privacy · provable security · symmetric encryption

Shay Gueron[1] and Yehuda Lindell[2]

[1] Department of Mathematics, University of Haifa, and Intel Corporation, Israel Development Center, Israel
shay@math.haifa.ac.il
[2] Department of Computer Science, Bar Ilan University, Israel
lindell@biu.ac.il

Abstract. Authenticated encryption schemes guarantee both privacy and integrity, and have become the default level of encryption in modern protocols. One of the most popular authenticated encryption schemes today is AES-GCM due to its impressive speed. The current CAESAR competition is considering new modes for authenticated encryption that will improve on existing methods. One property of importance that is being considered more today is due to the fact that the nonce or IV repeats, then this can have disastrous effects on security. A (full) nonce misuse-resistant authenticated encryption scheme has the property that if the *same* nonce is used to encrypt the *same* message twice, then the same ciphertext is obtained and so the fact that the same message was

Robust Encryption

Michel Abdalla[1] Mihir Bellare[2] Gregory Neven[3]

Abstract

We provide a provable-security treatment of "robust" encryption. Robustness means it is hard to produce a ciphertext that is valid for two different users. Robustness makes explicit a property that has been implicitly assumed in the past. We argue that it is an essential conjunct of anonymous encryption. We show that natural anonymity-preserving ways to achieve it, such as adding recipient identification information before encrypting, fail. We provide transforms that do achieve it, efficiently and provably. We assess the robustness of specific encryption schemes in the literature, providing simple patches for some that lack the property. We explain that robustness of the underlying anonymous IBE scheme is essential for PEKS (Public Key Encryption with Keyword Search) to be consistent (meaning, not have false positives), and our work provides the first generic conversions of anonymous IBE schemes to consistent (and secure) PEKS schemes. Overall our work enables safer and simpler use of encryption.

Message Franking via
Committing Authenticated Encryption*

Paul Grubbs[1], Jiahui Lu[2], and Thomas Ristenpart[1]

[1] Cornell Tech [2] Shanghai Jiao Tong University

Abstract

We initiate the study of message franking, recently introduced in Facebook's end-to-end encrypted message system. It targets verifiable reporting of abusive messages to Facebook without compromising security guarantees. We capture the goals of message franking via a new cryptographic primitive: compactly committing authenticated encryption with associated data (AEAD). This is an AEAD scheme for which a small part of the ciphertext can be used as a cryptographic commitment to the message contents. Decryption provides, in addition to the message, a value that can be used to open the commitment. Security for franking mandates more than that required of traditional notions associated with commitment. Nevertheless, and 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

Many ways to misuse and misunderstand AEADs

Our Approach

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?

4. We developed of multiple (symbolic) models to address the attack vector classes

Model it

5. We conducted case studies to show usefulness and feasibility of the new models
   - All case studies were analyzed completely automatic under all models

Test the model

AEAD Security in practice

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

- Integrity & Privacy
- Collision Resistance
- Nonce Reuse Resistance

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

✓ : 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.

Our theoretical models of AEAD weaknesses

Weaknesses in the main classes:

- Integrity & Privacy weakness
- Collisions
- Nonce Reuse

For completion

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

Case Study Methodology: Two Approaches

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Targeted Approach:

Check the protocol in the closest scenario from the real world

Preemptive Approach:

Check the protocol in all possible AEAD threat models

Case Study Methodology: Two Approaches

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

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	✓	✗	✗ Forgeability + xor of plaintexts
ChaCha20-Poly1305	✓	✗	✗ Xor of plaintexts
OCB3	✓	✗	✗ Forgeability + equality of blocks
EtM (unrelated keys)	✓	✗	✗ Encryption dependent
AES-CCM	✓	•	✗ Xor of plaintexts
AES-EAX	✓	•	✗ Xor of plaintexts
EtM (related keys)	✓	✓	✗ Encryption dependent
CAU-C4	✓	✓	✗ Forgeability + Xor of plaintexts
AES-GCM-SIV	✓	✗	✓
CAU-SIV-C4	✓	✓	✓

✓ : 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.

Case Study Methodology: Two Approaches

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

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

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	Tag	Collision
Time	2s	<1s	1s

Case Studies: Preemptive Approach

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

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!

Take-Away and Summary

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Formal Methods are useful in Protocol Design and Analysis!

New Insight when using Authenticated Encryption within Protocols:

- New relations between AEAD properties
- Classification of Protocol vulnerabilities caused by AE
  - May be useful for *draft-irtf-cfrg-aead-properties*

https://tamarin-prover.github.io/

(First!) Automated analysis of protocols that rely on AEADs

- Useful during protocol design
- Automatic detection of vulnerabilities/unwanted behavior caused by AEAD
- Extendable!

Alexander Dax: alexander.dax@cispa.de

Artifact: https://github.com/AutomatedAnalysisOf/AEADProtocols

Paper: https://www.usenix.org/conference/usenixsecurity23/presentation/cremers-protocols

Usenix 2023 Distinguished Paper Award!

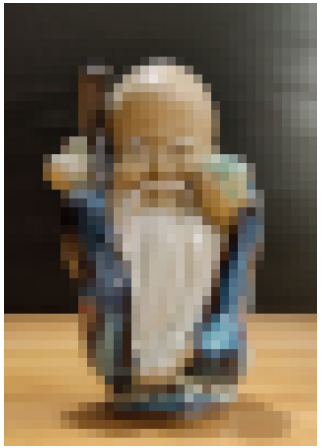
Formal security protocol analysis

Since early 1990's: **two main approaches**:

Reality

Computational

Prove probability of attack is negligible
Detailed models of encryption / signature



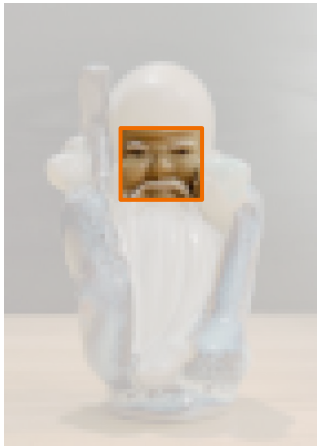
Symbolic

Focus on logical parts of the protocol design
Treat encryption / signature as black box

Formal security protocol analysis

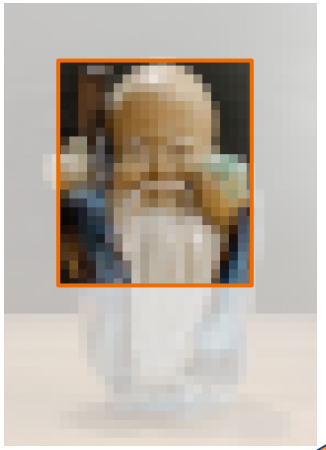
Since early 1990's: **two main approaches**:

Reality



Computational

Prove probability of attack is negligible
Detailed models of encryption / signature



Symbolic

Focus on logical parts of the protocol design
Treat encryption / signature as black box

Our AEAD analysis using the Tamarin prover

Classify AEAD notions and attacks

Gather relations between the existing AEAD notions and properties …

…and prove the missing ones

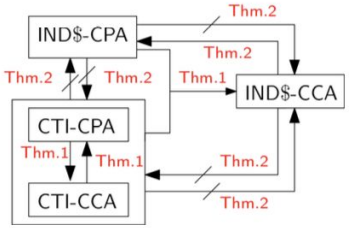


Figure 3: The relation between integrity and privacy for AEAD.

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

- Integrity & Privacy
- Collision Resistance
- Nonce Reuse