University of Haifa, January 2021

Key commitment and Multi Key Collision Attacks

Uri Ariel Yahalom* Shay Gueron†

Abstract

In this report we examine key commitment in Authenticated encryption and vulnerabilities that arise when it is not used exactly as designed. Recent research shows new class of attacks such as partitioning oracles which arise when AE schemes are not committing with respect to their keys. As key commitment is not part of AE's design goal, AE schemes in general do not satisfy it.

We show an adaptive chosen ciphertext attack that utilizes key multi-collision against widely used AEAD schemes, including AES-GCM, XSalsa20/Poly1305, and ChaCha20/Poly1305, to build a partitioning oracle.

We also discuss an early implementation of the OPAQUE protocol (a protocol for password-based key exchange) that is vulnerable to partitioning oracle.

*Department of Computer Science, University of Haifa.

†Department of Management, University of Haifa.

1 Background

Authenticated Encryption

AES-GCM

AES-GCM is an AEAD scheme that composes AES in counter mode with a specially designed MAC. It uses an XOR-universal hash function called GHASH. Encryption takes in a nonce N, an AES key K, associated data AD, and plaintext M. and it outputs a ciphertext $C_1, \ldots, C_n$ and an authentication tag T. The ciphertext blocks $C_1, \ldots, C_n$ are generated using counter mode with E, and the tag T is computed by applying GHASH to AD and $C_1, \ldots, C_n.$ Decryption also computes the tag, compares it with T, and, if successful, outputs the counter-mode decryption of the ciphertext blocks.

2 Key Commitment

Key commitment guarantees that a ciphertext can only be decrypted under the same key it was encrypted with. If we are to find a ciphertext that decrypts into two valid plaintexts under two different keys do not commit with respect to the key.

Key commitment was initially studied by Farshim et al. [FOR17] and while it might seem like an academic pursuit, Dodis et al. [DGRW18] and Grubbs et al. [GLR17a] show how to exploit AEADs that do not commit to their key. Nevertheless, AEAD key commitment has not received the required attention and can be overlooked in deployment.

A committing encryption scheme is a scheme for which it is computationally unfeasible to find two keys and a ciphertext that decrypts under both. Security standards for committing AEADs were first formalized by Farshim et al. [FOR17].

3 Multi Key Collision Attacks

Multi Key Collision Attacks is an attack where we find a ciphertext - C that decrypts under k different keys.
In practice, to perform a multi key collision attack against AES-GCM we need to solve a system of linear equations. This is possible because of the algebraic properties of the universal hashing in AES-GCM.

4 Partitioning Oracles

The design of encryption historically separated the goals of confidentiality and authenticity, which led to widespread deployment of encryption schemes vulnerable to chosen ciphertext attacks (CCA).
Subsequently, researchers showed how to exploit CCAs to recover plaintext data, most notably via padding and format oracle attacks As a result, cryptographers now advocate the use of authenticated encryption with associated data (AEAD) schemes and CCA-secure public key encryption. There has since been a shift to adopt fast CCA-secure schemes, notably AES-GCM, and XSalsa20/Poly1305.
Such schemes do not target being committing. Thus far, key commitment has not been considered an essential security goal for most cryptographic applications. This is perhaps because attacks exploiting key collision have arisen in relatively niche applications like message franking for encrypted messages.
Grubbs et al. introduce partitioning oracle attacks, a new type of CCA in password-authenticated key exchange (PAKE). A partitioning oracle arises when an attacker can:

1. efficiently prepare ciphertexts that will decrypt under a large number of keys

2. submit those ciphertexts to an oracle that tells whether decryption succeeds or fails.

This enables gaining information about the password.

References

Julia Len, Paul Grubbs and Thomas Ristenpart. Partitioning Oracle Attacks.

Ange Albertini, Thai Duong, Shay Gueron, Stefan Kölbl, Atul Luykx and Sophie Schmieg. How to Abuse and Fix Authenticated Encryption Without Key Commitment.

Appendix

The asterisk means that these divisions are not numbered.

How to write Mathematics

This section is completely redundant with the text. Do not do that. This is just an example.
LaTeX is great at typesetting mathematics. Let $X_1, X_2, \ldots, X_n$ be a sequence of independent and identically distributed random variables with $\mathrm{E}[X_i] = \mu$ and $\mathrm{Var}[X_i] = \sigma^2 < \infty$, and let

$$S_n = \frac{X_1 + X_2 + \cdots + X_n}{n} = \frac{1}{n} \sum_{i}^{n} X_i$$

denote their mean. Then as n approaches infinity, the random variables $\sqrt{n}(S_n - \mu)$ converge in distribution to a normal $\mathcal{N}(0, \sigma^2)$.

How to create Sections and Subsections

Use section and subsections to organize your document. Simply use the section and subsection buttons in the toolbar to create them, and we'll handle all the formatting and numbering automatically.