May 2020

Energy Efficient In-line Encryption With Selective Round Masking

Anonymous

Energy Efficient In-line Encryption With Selective Round Masking

ABSTRACT

Side channel protection imposes substantial area, performance, and/or energy overhead, rendering such hardware unsuitable for devices that have space or battery constraints, e.g., head-mounted display (HMD) devices. To safeguard user data in such devices, energy efficient encryption techniques are necessary. This disclosure describes an in-line encryption engine that uses selective masking. The first and last rounds of encryption are accorded maximum protection by incorporating all masking features, while intermediate rounds are only partially masked at steps that are determined as likely vulnerable, or are left unmasked. Selective round masking in this manner provides data protection with low cost, and is suitable for use in devices with space or battery constraints, such as HMD devices.

KEYWORDS

- In-line encryption
- Selective masking
- Advanced encryption standard (AES)
- Side-channel attack (SCA)
- Head-mounted display (HMD)
- Virtual reality
- Augmented reality
- VR goggles

BACKGROUND

Encryption is important for content protection in augmented reality (AR) and virtual reality (VR) devices to safeguard user data, and to enable seamless connectivity and data flow

that is imperative to deliver a high quality user experience. Side-channel attack (SCA) resistant encryption hardware is becoming commonplace in security platforms to mitigate leakage of private information via passive channels such as electromagnetic emission, battery power consumption, etc.

However, side channel protection comes at significant area, performance, and/or energy overhead, rendering such hardware unsuitable for devices that have space and/or battery constraints, e.g., head-mounted display (HMD) devices.

DESCRIPTION

This document describes techniques that achieve side-channel protection for in-line acceleration engines with a low overhead. By lowering encryption energy, the described techniques help augmented reality (AR) platforms operate within a limited power budget. Further, the techniques also reduce attack surface by enabling encryption of more content, including data from multiple sensors, that are beyond the scope of current encryption strategy owing to high power requirements.

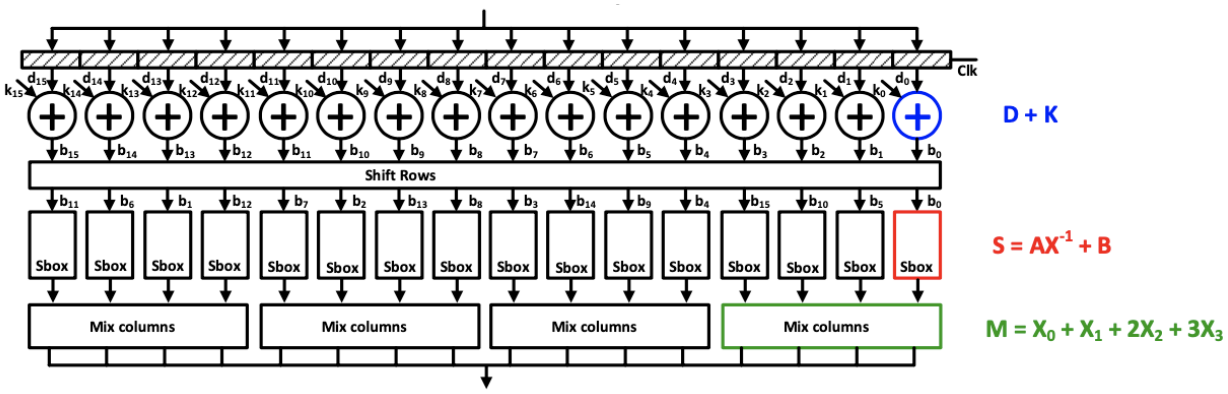

Fig. 1: AES with unmasked round datapath

AES is the de facto encryption standard for content protection. High throughput in-line engines typically include multiple stages of AES hardware, wherein each stage (also called AES

round) includes identical logic for a set of 4 operations. These 4 operations termed as add-key, shift-row, substitute-byte (Sbox), and mix-columns are shown in Fig. 1.

In conventional, non-SCA engines, the key interacts with the plain text in a deterministic way across the 10 rounds resulting in a specific pattern of switching activity in the AES datapath. An SCA protected engine amalgamates the input data using a random number before interaction with the key, thereby randomizing the switching-activity and corresponding energy-dissipation in the hardware.

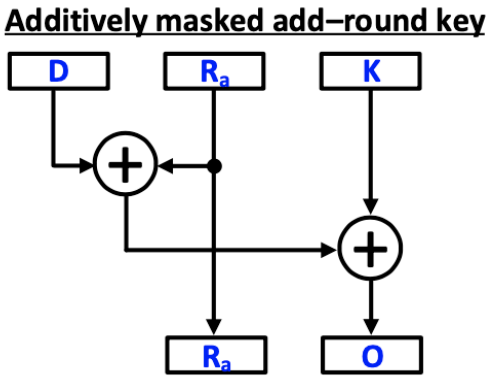

Fig. 2: Additively masked add-round key

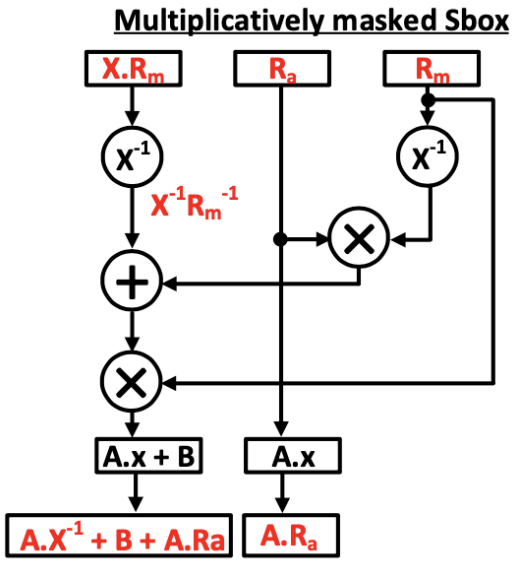

Fig. 3: Multiplicatively masked Sbox

For example, as shown in Fig. 2, in key addition, a random salt R_a gets added to input data D prior to the addition of the encryption key K. The datapath keeps track of this random salt to ensure accurate recovery of the actual data in the end. Additive masking is not computationally feasible in Sbox because of the presence of an inverse operation that makes mask reversal impractical. Instead a multiplicative mask is used as shown in Fig. 3.

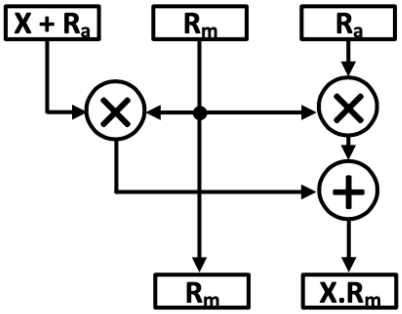

Fig. 4: Additive to multiplicative mask translation

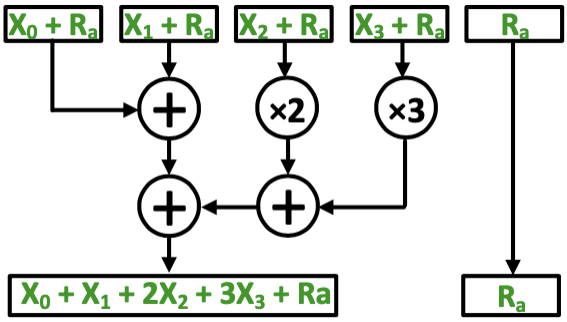

Fig. 5: Additively masked Mixcolumns

Furthermore, a mask translation unit is required in the round logic to convert the additive mask into a multiplicative mask, as shown in Fig. 4. Although the Sbox unit consumes data that is multiplicatively masked, extra steps are incorporated that translate the mask into additive format that is seamlessly consumed by the mix-columns unit as shown in Fig. 5. The presence of additional masking logic incurs area, performance, and power overhead.

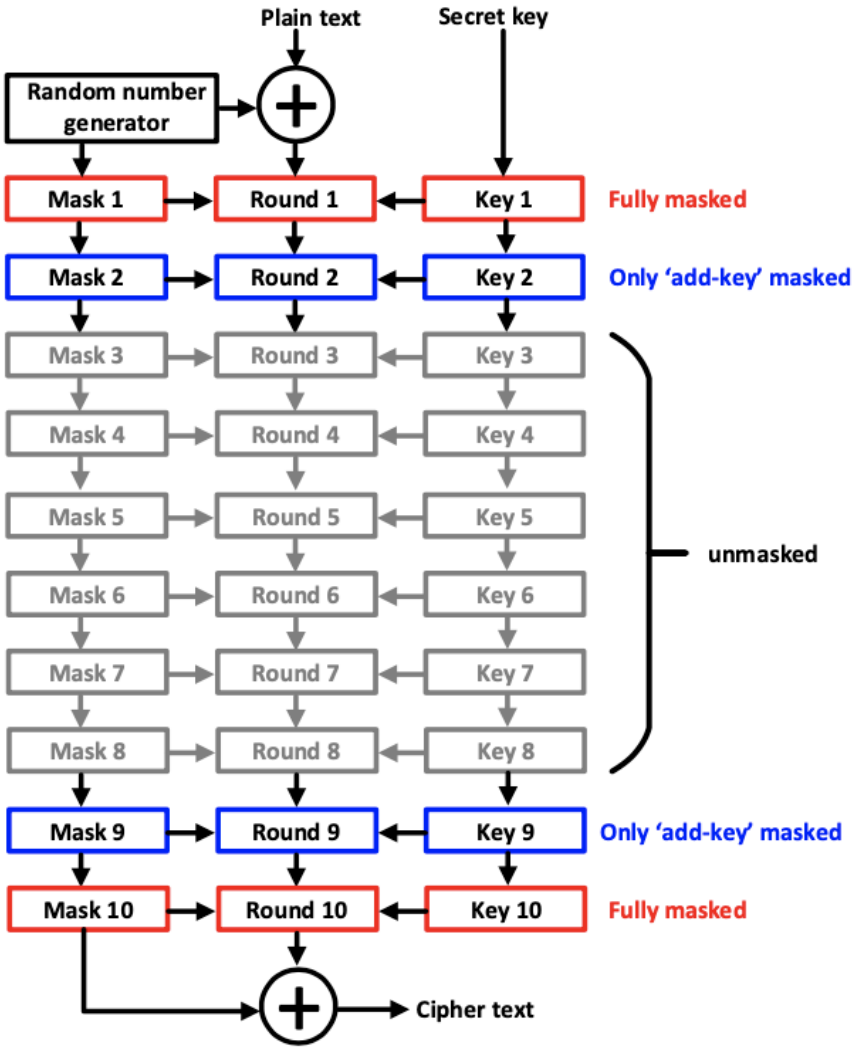

Fig. 6: Selectively masked encryption engine

State-of-art high-throughput in-line AES encryption engines unroll the hardware into 10 rounds where each round is a replica template feeding the next round. To incorporate SCA protection, the hardware incurs extra logic overhead. In contrast, the techniques described herein, shown in Fig. 6, use a novel datapath that uses asymmetric rounds.

SCA procedures are more effective at hardware points that are logically close to observable data since these points provide the best model with fewest unknowns for an attacker to observe the effect of secret key. For in-line engines the first and last rounds are typical

candidates for SCA analysis because of their proximity to user injected plain text and received cipher text respectively.

Hence, per techniques described herein, maximum protection is provided to these rounds by incorporating all the masking features described above. Rounds midway are the most difficult to attack, and hence are unmasked which saves power. Other rounds midway are only partially masked at logic that are most prone to leaking secrets, e.g., the "add-round key" step. Although the figure above shows one instantiation of the proposed approach, other implementations of selectively masked rounds are possible by assessing secret leakage in various stages for each specific design. This can be done using standard correlation analysis that provides a metric quantifying the degree of secret leakage in various rounds.

CONCLUSION

This disclosure describes an in-line encryption engine that uses selective masking. The first and last rounds of encryption are accorded maximum protection by incorporating all masking features, while intermediate rounds are only partially masked at steps that are determined as likely vulnerable, or are left unmasked. Selective round masking in this manner provides data protection with low cost. The described design is suitable for use in devices with space or battery constraints, such as HMD devices.