Leakage Resilience of the ISAP Mode: a Vulgarized Summary

Christoph Dobraunig and Bart Mennink

Digital Security Group, Radboud University, Nijmegen, The Netherlands
cdobraunig@cs.ru.nl, b.mennink@cs.ru.nl

Abstract. ISAP is a lightweight authenticated encryption scheme that puts its focus on achieving protection against implementation attacks using a minimal amount of resources. The scheme solely relies on cryptographic permutations as building blocks, which can be implemented by iterating a single round function just using different constants per round. The clever design of ISAP aims to provide protection against side-channel attacks like (higher-order) differential power analysis and implementations attacks even in the absence of costly implementation-level countermeasures like masking. In particular, the protection against side-channel attacks just requires implementations which prohibit attacks that just utilize power traces from up to two different inputs, e.g, simple power analysis and template attacks. In this note, we summarize how two disjoint works on leakage resilience, namely that on keyed duplexes and that on the suffix keyed sponge, can be combined to obtain a bound on the leakage resilience of the ISAP construction.

1 Introduction

Isap is a family of nonce-based authenticated ciphers specifically designed to withstand implementation attacks, especially providing robustness against passive side-channel attacks. It combines different sponge constructions, called IsapRK, IsapEnc, and IsapMAC to limit leakage incurred by leaky implementations. Its original mode was published at FSE 2017 [6], and it is currently in submission to the NIST lightweight cryptography standardization process [13]. A specification of Isap is given in Section 2.

The authors of Isap did not deliver a security proof. However, they gave an intuition as to why Isap might be leakage resilient. Unfortunately, proving leakage resilience of Isap turned out to be more subtle than expected. One of the reasons is that IsapMAC is structurally different from IsapRK and IsapEnc. The functions IsapRK and IsapEnc are instances of a keyed duplex that *instantiate the state with a key* and subsequently evolve the state by duplexing calls with extraction or absorption. The function IsapRK, on the other hand, first absorbs data and *finalizes the state with a key*.

In two recent articles, Dobraunig and Mennink (DoMe) set out to perform a leakage resilience analysis of these two components. In [7], DoMe proved leakage resilience of the generalized keyed duplex mode. This mode in particular covers IsapRK and the stream encryption within IsapEnc. DoMe showed how these two can be combined to obtain confidentiality of a variant of Isap. In [8], DoMe introduced and formalized the suffix keyed sponge and proved its leakage resilience. The authentication part of Isap, IsapMAC, is a special type of suffix keyed sponge.

These two works [7, 8] lead to leakage resilience of Isap, with two caveats:

- The demonstration of how the duplex can be used to achieve confidentiality in [7] is slightly different from how Isap performs encryption. The composition has yet to be described in detail;
- The security proof of the suffix keyed sponge abstracts the key absorption. In Isap, this key absorption is done by IsapRK, which is also called by IsapEnc. This means that we cannot directly conclude security of Isap from the disjoint results of [7] and [8], but the combination must be spelled out.

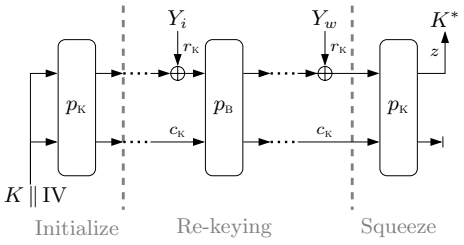
In this brief note, we show how the leakage resilience of the keyed duplex and the leakage resilience of the suffix keyed sponge accumulate to the leakage resilience of the ISAP mode. The ingredients of keyed duplex security are summarized in Section 3, and those on suffix keyed sponge security in Section 4. The main result on the ISAP mode is stated and discussed in Section 5. The note is purposely high-level: in the body of this note we omit all technicalities and use [7, 8] as a black-box insofar possible. Nevertheless, a more formal reasoning is included, but only in Appendix A. Section 6 contains an interpretation of the results.

Finally, we remark that Guo et al. (GPPS) [11] independently constructed a security argument for ISAP. It follows a different strategy, and henceforth resulted in different bounds and underlying assumptions. We elaborate on the argument of GPPS in Section 7.

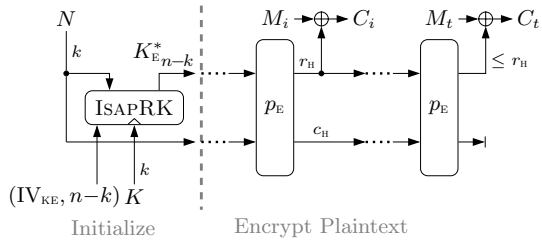
2 ISAP

ISAP is specified by a security parameter k. Authenticated encryption of ISAP gets as input a key $K \in \{0,1\}^k$, a nonce $N \in \{0,1\}^k$, associated data $A \in \{0,1\}^*$, and a message $M \in \{0,1\}^*$. It outputs a ciphertext $C \in \{0,1\}^{|M|}$ and a tag $T \in \{0,1\}^k$. It is an encrypt-then-MAC design. Encryption ISAPENC is depicted in Figure 1b and message authentication ISAPMAC in Figure 1c. Both functions internally use a rekeying function ISAPRK, which is depicted in Figure 1a. We remark that, although we have sticked to the figures of the specification of ISAP of Dobraunig et al. [5], we have simplified notation here and there to suit the readability of this short note.

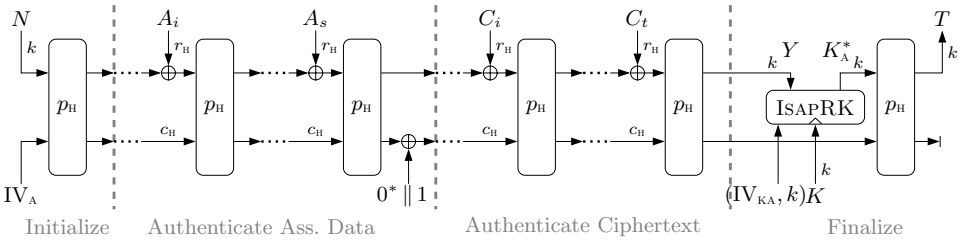
ISAP comes with four variants, two of which have $n = 320$ and two of which have $n = 400$. In any case, the security level is $k = 128$. The compression in ISAPRK occurs at rate $r_{\mathrm{K}} = 1$. The hashing capacity satisfies $c_{\mathrm{H}} = 2k = 256$ for all variants, and the hashing rate subsequently satisfies $r_{\mathrm{H}} = n - 2k$. In our bounds, we will keep n and k as parameters, and express $r_{\mathrm{K}}, c_{\mathrm{K}}, r_{\mathrm{H}}, c_{\mathrm{H}}$ as function of these.



(a) ISAPRK, with $(\mathrm{IV}, z) = (\mathrm{IV}_{\mathrm{KE}}, n-k)$ if called by ISAPENC and $(\mathrm{IV}, z) = (\mathrm{IV}_{\mathrm{KA}}, k)$ if called by ISAPMAC



(b) ISAPENC



(c) ISAPMAC

Fig. 1: ISAP authenticated encryption

3 Ingredient 1: Duplex

The duplex was introduced by Bertoni et al. [3], and was generalized subsequently by Mennink et al. [12] and Daemen et al. [4]. DoMe [7] started from the generalized construction and proved its leakage resilience. They demonstrated how *two specific types of duplex*, that of "gaining entropy" and that of "maintaining entropy", combined to leakage resilient stream encryption. This separation was inspired by the separation of IsapRK and of the stream encryption within IsapEnc. However, in IsapEnc the composition is slightly different, and in addition, IsapRK is not only used for IsapEnc but also for IsapMAC.

Nevertheless, we can take inspiration of the separation outlined by DoMe [7] and conclude leakage resilience for IsapRK and for IsapEnc (with idealized IsapRK). The results are summarized in Section 3.1 and Section 3.2.

3.1 Leakage Resilience of IsapRK

Transforming DoMe's result [7, Corollary 1] to Isap, we obtain that IsapRK is a leakage resilient duplex, as long as $p_{\text{K}} = p_{\text{B}}$ is a random permutation.

Proposition 1. *Under the assumption that $p_{\text{K}} = p_{\text{B}}$ is a random permutation,* IsapRK *is a leakage resilient duplex up to a security bound of the order*

$$\mathcal{O}\left(\frac{kqP}{2^{n-4\lambda}} + \frac{P}{2^{k-2\lambda}}\right),$$

where q denotes the amount of construction queries, P the amount of permutation queries, and λ the maximum amount of leakage per permutation evaluation.

3.2 Leakage Resilience of IsapEnc

Transforming DoMe's result [7, Corollary 2] to Isap, we obtain that the plaintext encryption part of IsapEnc is a leakage resilient duplex, as long as p_{E} is a random permutation and the keys coming from IsapRK have sufficiently high min-entropy.

Proposition 2. *Under the assumption that p_{E} is a random permutation and* IsapRK *results in keys with sufficiently high min-entropy, the plaintext encryption part of the function* IsapEnc *is a leakage resilient stream encryption function up to a security bound of the order*

$$\mathcal{O}\left(\frac{qQ}{2^{n-k-2\lambda}} + \frac{P^2}{2^n}\right),$$

where q denotes the amount of construction queries, Q the total amount of message blocks, P the amount of permutation queries, and λ the maximum amount of leakage per permutation evaluation.

4 Ingredient 2: Suffix Keyed Sponge

The suffix keyed sponge (SuKS) was introduced and proven to be a leakage resilient PRF by DoMe [8]. There are three subtle differences between the suffix keyed sponge and IsapMAC:

(i) SuKS initializes the state with the initial value 0, whereas IsapMAC takes IV_{A};
(ii) SuKS takes an arbitrarily-long input and compresses it over the rate. In contrast, IsapMAC takes two arbitrarily-long inputs and sacrifices one bit of the capacity for domain separation;
(iii) SuKS is proven for arbitrary key absorption at the end, whereas IsapMAC calls IsapRK.

The former two do not affect the inheritance of DoMe [8] to Isap, the only difference is that the capacity reduces by 1. With respect to the latter point, we remark that due to Proposition 1, IsapRK turns out to be a sufficiently leakage resilient key absorption function in the terminology of DoMe [8].

Transforming DoMe's result [8, Theorem 3] to Isap, we obtain that IsapMAC is a leakage resilient PRF, as long as p_{H} is a random permutation and IsapRK is a sufficiently leakage resilient secure random function.

Proposition 3. *Under the assumption that p_{H} is a random permutation and* IsapRK *is strongly protected, the function* IsapMAC *is a leakage resilient PRF up to a security bound of the order*

$$\mathcal{O}\left(\frac{P}{2^{k-cst\cdot\lambda}}\right),$$

where P denotes the amount of permutation queries, and λ the maximum amount of leakage per permutation evaluation. Here, cst is a small constant.

5 Leakage Resilience of ISAP

The independent and disjoint results from DoMe culminate to a complete security proof of the Isap mode as an authenticated encryption scheme. Here, we will only give the intuition. A more detailed proof is included in Appendix A.

Theorem 1. *Under the assumption that $p_{\text{K}} = p_{\text{B}}$, p_{E}, and p_{H} are three mutually independent random permutations,* Isap *is a leakage resilient authenticated encryption scheme up to a security bound of the order*

$$\mathcal{O}\left(\frac{qQ}{2^{n-k-2\lambda}} + \frac{P}{2^{k-cst\cdot\lambda}} + \frac{q_v}{2^k}\right),$$

where q denotes the amount of construction queries, Q the total amount of message blocks, q_v the total number of verification attempts, P the amount of permutation queries, and λ the maximum amount of leakage per permutation evaluation. Here, cst is a small constant.

Proof (sketch). Although the proof follows that of [7, Theorem 2] for a large amount, slight differences occur in the context of authenticated encryption, and more detailed if IsapRK is used for both IsapEnc and IsapMAC.

The first step in the proof is to note that IsapRK is in fact a leakage resilient duplex, cf., Proposition 1. This means that we can replace it by a random leakage resilient duplex in our construction, at the cost of the bound of Proposition 1. The reduction step is possible as the permutation it is based on is generated independently from the permutations on which IsapEnc and IsapMAC are based.

Note that, in fact, IsapRK is called by both IsapEnc and IsapMAC, but these calls happen for different IV's. As we have replaced IsapRK by a random duplex, it behaves independently when called by IsapEnc or by IsapMAC. This means that we end up with a neat separation: IsapEnc is instantiated with random permutation p_{E} and calls the ideal leakage resilient rekeying duplex for $\text{IV} = \text{IV}_{\text{KE}}$, whereas IsapMAC is instantiated with random permutation p_{H} and calls the ideal leakage resilient rekeying duplex for $\text{IV} = \text{IV}_{\text{KA}}$.

This means that we can rely on Proposition 2 and Proposition 3 independently. For both propositions, the premise on IsapRK is met (as we have replaced it with an ideal leakage resilient rekeying duplex), and we obtain that encryption IsapEnc behaves like an ideal leakage resilient duplex (de facto behaving perfectly ideal) and that authentication IsapMAC behaves like a random function (de facto behaving perfectly ideal).

What remains is to consider the advantage of the adversary in forging a tag for a randomized scheme. This advantage is around 2^{-k} for each attempt. □

6 Interpretation

We stress that the work assumes uniform randomness and mutual independence of $p_{\text{K}} = p_{\text{B}}$, p_{E}, and p_{H}. Therefore, our result only applies to the *mode* of Isap, it does not mean unconditional security of the Isap authenticated encryption scheme. On the upside, the result implies that any attack against Isap must take at least some property of the permutations in mind. One property that might be considered is that the instances of Isap do not strictly use four structural different permutations, but use similar permutations instead.

The result shows leakage resilience of the Isap authenticated encryption scheme under the assumption that only the cryptographic functionalities, e.g., the permutations, leak information. We have assumed that no other aspect of the scheme leaks. Caution must be paid for tag verification: if the tag verification (a non-cryptographic operation) is not done in a leakage resilient manner, this may leak information and henceforth invalidate the results (see also [2,11]). Therefore, one should make sure that tag verification is performed in a leakage resilient manner. The designers of Isap [5] suggest to counter this by making one additional permutation call during the verification. In this case, T and T' are computed and transmitted as normal, but instead of a direct comparison, e.g., $\text{left}_k(p_{\text{H}}(T'\|0^{n-k}))$ is compared with $\text{left}_k(p_{\text{H}}(T\|0^{n-k}))$ first.

7 Comparison with GPPS

GPPS independently considered leakage resilience of the Isap mode, in a 20-May-2019 updated version of their ePrint article [11]. They start from the TEDTSponge construction, and sketch how the analysis generalizes to Isap. Their approach to treating confidentiality (i.e., the analysis of IsapEnc) is almost identical to the approach suggested by DoMe [7, Theorem 2] and adopted in Theorem 1. For the authenticity of Isap (i.e., the analysis of IsapMAC), GPPS likewise first idealize IsapRK, but the subsequent analysis of IsapMAC is only very briefly sketched [11, Appendix H], and misses the rigor and detail of the suffix keyed sponge analysis of DoMe [8]. Note that GPPS indicate that their proof is a sketch and thus, their bounds are described in big $\mathcal{O}$ notation without supporting computation.

Further differences between our proof and that of GPPS surface at the security model and assumptions. In our model, we allow the adversary to obtain leakage data, but the challenge queries do not leak (see Section A.1). GPPS adopt a model where even the challenge queries leak, but depart from the real-or-random security model to achieve this. The difference is debatable, see GPPS [11, Section 2]. A second difference is on the assumption on leakage. We consider a bounded leakage model, that upper bounds the amount of information that an attacker learns by λ, whereas GPPS assume hard-to-invert leakages.

Overall, one can say that the approaches are different and complementary.

Acknowledgments. Christoph Dobraunig is supported by the Austrian Science Fund (FWF): J 4277-N38. Bart Mennink is supported by a postdoctoral fellowship from the Netherlands Organisation for Scientific Research (NWO) under Veni grant 016.Veni.173.017.

References

1. Barwell, G., Martin, D.P., Oswald, E., Stam, M.: Authenticated Encryption in the Face of Protocol and Side Channel Leakage. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017. LNCS, vol. 10624, pp. 693–723. Springer (2017)
2. Berti, F., Guo, C., Pereira, O., Peters, T., Standaert, F.X.: TEDT, a Leakage-Resilient AEAD mode for High (Physical) Security Applications. Cryptology ePrint Archive, Report 2019/137 (2019)
3. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: Duplexing the Sponge: Single-Pass Authenticated Encryption and Other Applications. In: Miri, A., Vaudenay, S. (eds.) SAC 2011. LNCS, vol. 7118, pp. 320–337. Springer (2011)

4. Daemen, J., Mennink, B., Van Assche, G.: Full-State Keyed Duplex with Built-In Multi-user Support. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017. LNCS, vol. 10625, pp. 606–637. Springer (2017)
5. Dobraunig, C., Eichlseder, M., Mangard, S., Mendel, F., Mennink, B., Primas, R., Unterluggauer, T.: ISAP v2. Submission to NIST Lightweight Cryptography (2019)
6. Dobraunig, C., Eichlseder, M., Mangard, S., Mendel, F., Unterluggauer, T.: ISAP - Towards Side-Channel Secure Authenticated Encryption. IACR Trans. Symmetric Cryptol. 2017(1), 80–105 (2017)
7. Dobraunig, C., Mennink, B.: Leakage Resilience of the Duplex Construction. In: Galbraith, S., Moriai, S. (eds.) ASIACRYPT 2019. LNCS (2019), to appear
8. Dobraunig, C., Mennink, B.: Security of the Suffix Keyed Sponge. Cryptology ePrint Archive, Report 2019/573 (2019)
9. Dodis, Y., Pietrzak, K.: Leakage-Resilient Pseudorandom Functions and Side-Channel Attacks on Feistel Networks. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 21–40. Springer (2010)
10. Faust, S., Pietrzak, K., Schipper, J.: Practical Leakage-Resilient Symmetric Cryptography. In: Prouff, E., Schaumont, P. (eds.) CHES 2012. LNCS, vol. 7428, pp. 213–232. Springer (2012)
11. Guo, C., Pereira, O., Peters, T., Standaert, F.X.: Towards Lightweight Side-Channel Security and the Leakage-Resilience of the Duplex Sponge. Cryptology ePrint Archive, Report 2019/193 (2019)
12. Mennink, B., Reyhanitabar, R., Vizár, D.: Security of Full-State Keyed Sponge and Duplex: Applications to Authenticated Encryption. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9453, pp. 465–489. Springer (2015)
13. National Institute of Standards and Technology (NIST): Submission requirements and evaluation criteria for the lightweight cryptography standardization process (Aug 2018)
14. Pietrzak, K.: A Leakage-Resilient Mode of Operation. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 462–482. Springer (2009)
15. Standaert, F.X., Pereira, O., Yu, Y., Quisquater, J.J., Yung, M., Oswald, E.: Leakage Resilient Cryptography in Practice. In: Sadeghi, A.R., Naccache, D. (eds.) Towards Hardware-Intrinsic Security - Foundations and Practice, pp. 99–134. Information Security and Cryptography, Springer (2010)
16. Yu, Y., Standaert, F.X., Pereira, O., Yung, M.: Practical leakage-resilient pseudorandom generators. In: Al-Shaer, E., Keromytis, A.D., Shmatikov, V. (eds.) CCS 2010. pp. 141–151. ACM (2010)

A Detailed Version of the Proof

A.1 Security Model

We consider security of $\textsc{Isap} = (\mathcal{E}, \mathcal{D})$ in the random permutation model. We consider a simplified setting where $p_1 := p_{\text{K}} = p_{\text{B}}$, $p_2 := p_{\text{E}}$, and $p_3 := p_{\text{H}}$ are uniformly randomly drawn from the set of all n-bit permutations: $p_1, p_2, p_3 \xleftarrow{\$} \mathsf{perm}(n)$. Let $K \xleftarrow{\$} \{0,1\}^k$. Let $\$_{*+k}$ be a function that for each (N, A, M) outputs a uniform random string of length $|M| + k$ bits (noting that a nonce should never be repeated), and let $\perp$ be a function that always returns $\perp$.

In the black-box security model, one would consider an adversary that has access to either $(\mathcal{E}_K^{\boldsymbol{p}}, \mathcal{D}_K^{\boldsymbol{p}}, \boldsymbol{p}^{\pm})$ in the real world or $(\$_{*+k}, \perp, \boldsymbol{p}^{\pm})$ in the ideal world, where $\boldsymbol{p} = (p_1, p_2, p_3)$ and where "$\pm$" stands for bi-directional query access:

$$\mathbf{Adv}^{\text{ae}}_{\textsc{Isap}}(\mathcal{A}) = \Delta_{\mathcal{A}}\left(\mathcal{E}_K^{\boldsymbol{p}}, \mathcal{D}_K^{\boldsymbol{p}}, \boldsymbol{p}^{\pm}\ ;\ \$_{*+k}, \perp, \boldsymbol{p}^{\pm}\right) .$$

In case of leakage resilience, we adopt the conventional approach of non-adaptive leakage resilience, e.g., [9, 10, 14–16], where the adversary has access to a leak-free version of the construction, which it has to distinguish from random, and a leaky version, which it may use to gather information. We assume that, a priori, any permutation evaluation within the leaky construction may leak information.

Formally, we obtain the following model, which follows Barwell et al. [1] with the difference that we consider security in the ideal permutation model. Let $\boldsymbol{p}, K, \$_{*+k}$ be as above. Let $\mathcal{L} = \{L : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^\lambda\}$ be a class of leakage functions, and for any leakage function $L \in \mathcal{L}$, define by $[\mathcal{E}_K^{\boldsymbol{p}}]_L$ (resp., $[\mathcal{D}_K^{\boldsymbol{p}}]_L$) an evaluation of $\mathcal{E}_K^{\boldsymbol{p}}$ (resp., $\mathcal{D}_K^{\boldsymbol{p}}$) where each permutation call within leaks λ bits of its input plus output. We now consider an adversary that *in addition* to the oracles in the black-box model has access to $[\mathcal{E}_K^{\boldsymbol{p}}]_L$ and $[\mathcal{D}_K^{\boldsymbol{p}}]_L$:

$$\mathbf{Adv}^{\text{nalr-ae}}_{\textsc{Isap}}(\mathcal{A}) = \max_{L \in \mathcal{L}} \Delta_{\mathcal{A}}\left([\mathcal{E}_K^{\boldsymbol{p}}]_L, [\mathcal{D}_K^{\boldsymbol{p}}]_L, \mathcal{E}_K^{\boldsymbol{p}}, \mathcal{D}_K^{\boldsymbol{p}}, \boldsymbol{p}^{\pm}\ ;\ [\mathcal{E}_K^{\boldsymbol{p}}]_L, [\mathcal{D}_K^{\boldsymbol{p}}]_L, \$_{*+k}, \perp, \boldsymbol{p}^{\pm}\right) . \quad (1)$$

The adversary is not allowed to make an encryption query (to the leaky or leak-free oracle) under a repeated nonce.

A.2 Multicollision Limit Function

Daemen et al. [4] introduced the multicollision limit function in the context of keyed sponge proofs. Let $q, n, s \in \mathbb{N}$ such that $s \leq n$. Consider the experiment of throwing q balls uniformly at random in 2^{n-s} bins, and denote by μ the maximum number of balls in any single bin. The multicollision limit function $\mu^q_{n-k,k}$ is defined as the smallest natural number x that satisfies

$$\mathbf{Pr}\left(\mu > x\right) \leq \frac{x}{2^s} .$$

Daemen et al. [4] also gave an in-depth analysis of the term $\mu^q_{n-k,k}$. The analysis is tedious, but the conclusion is that the term behaves as follows:

$$\mu^q_{n-k,k} \lesssim \begin{cases} n / \log_2\left(\dfrac{2^{n-s}}{q}\right) , & \text{for } q \lesssim 2^{n-s} , \\ n \cdot \dfrac{q}{2^{n-s}} , & \text{for } q \gtrsim 2^{n-s} . \end{cases}$$

A.3 Main Result

We present the main result on the leakage resilience of the ISAP mode. The result is stated with respect to the formalism of Section A.1.

Theorem 2. *Assume that $4 \leq k \leq n$, and $1 \leq \lambda \leq 2n$. Let $\boldsymbol{p} = (p_1, p_2, p_3) \xleftarrow{\$} \mathsf{perm}(n)^3$ and $K \xleftarrow{\$} \{0,1\}^k$. Let $\mathcal{L} = \{L : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^\lambda\}$ be a class of leakage functions. For any adversary making $q \geq 2$ queries with unique nonces for encryption queries with a total amount of Q plaintext blocks, and $P \leq 2^{n-1}$ primitive queries to each of p_1, p_2, p_3,*

$$\begin{aligned}\mathbf{Adv}^{\text{nalr-ae}}_{\text{ISAP}}(\mathcal{A}) \leq{}& \frac{4\binom{4+2kq+P}{2} + 2\binom{Q+P}{2} + 6\binom{P}{2}}{2^n} + \frac{2\binom{Q}{2}}{2^{n-\lambda}} + \frac{32kqP + 16k^2q^2}{2^{n-4\lambda}} \\ &+ \frac{2\mu_{k,n-k}^{2(P-q)}}{2^{n-k}} + \frac{2\mu_{k,n-k}^{2q} \cdot P}{2^{n-k-\lambda}} + \frac{2P + 2qQ}{2^{n-k-2\lambda}} \\ &+ \frac{8P^2}{2^{2k}} + \frac{4\mu_{2k,n-2k}^{Q} \cdot (P+1)}{2^{2k-2\lambda}} + \frac{q_v + 4}{2^k} + \frac{8P}{2^{k-2\lambda}} + \frac{2\mu_{n-k,k}^{2(P-q)} \cdot P}{2^{k-\lambda-\mu_{k,n-k}^{2(P-q)}\lambda}}\,.\end{aligned}$$

where q_v is the total number of verification attempts.

The proof is included in Section A.4.

A.4 Proof of Theorem 2

Formalization. Note that both encryption $\mathcal{E}$ and decryption $\mathcal{D}$ of ISAP can be specified as function of ISAPRK =: IR, ISAPENC =: IE, and ISAPMAC =: IM:

$$\begin{aligned}\mathcal{E}_K^{\boldsymbol{p}} &= \mathcal{E}^{\mathrm{IR}_K^{p_1}, \mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}}, \mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}\,, \\ \mathcal{D}_K^{\boldsymbol{p}} &= \mathcal{D}^{\mathrm{IR}_K^{p_1}, \mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}}, \mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}\,,\end{aligned}$$

where $\boldsymbol{K}^\star_{\mathrm{KE}}$ is defined as the output states of $\mathrm{IR}_K^{p_1}$ for $\mathrm{IV} = \mathrm{IV}_{\mathrm{KE}}$, and $\boldsymbol{K}^\star_{\mathrm{KA}}$ the output states of $\mathrm{IR}_K^{p_1}$ for $\mathrm{IV} = \mathrm{IV}_{\mathrm{KA}}$. Here, the * is used to explicitly remind of the fact that the keys come from $\mathrm{IR}_K^{p_1}$. Note that these values are, in particular, defined by the inputs to IE^{p_2} and IM^{p_3}.

Let $L \in \mathcal{L}$ be any leakage and $\mathcal{A}$ be any adversary. Our goal is to bound

$$\begin{aligned}&\Delta_{\mathcal{A}}\left([\mathcal{E}_K^{\boldsymbol{p}}]_L, [\mathcal{D}_K^{\boldsymbol{p}}]_L, \mathcal{E}_K^{\boldsymbol{p}}, \mathcal{D}_K^{\boldsymbol{p}}, \boldsymbol{p}^{\pm}\,;\, [\mathcal{E}_K^{\boldsymbol{p}}]_L, [\mathcal{D}_K^{\boldsymbol{p}}]_L, \$_{*+k}, \perp, \boldsymbol{p}^{\pm}\right) \\ =&\Delta_{\mathcal{A}}\Big(\Big[\mathcal{E}^{\mathrm{IR}_K^{p_1}, \mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}}, \mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}\Big]_L, \Big[\mathcal{D}^{\mathrm{IR}_K^{p_1}, \mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}}, \mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}\Big]_L, \mathcal{E}^{\mathrm{IR}_K^{p_1}, \mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}}, \mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}, \mathcal{D}^{\mathrm{IR}_K^{p_1}, \mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}}, \mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}, \boldsymbol{p}^{\pm}\,; \\ &\qquad\Big[\mathcal{E}^{\mathrm{IR}_K^{p_1}, \mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}}, \mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}\Big]_L, \Big[\mathcal{D}^{\mathrm{IR}_K^{p_1}, \mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}}, \mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}\Big]_L, \$_{*+k}, \perp, \boldsymbol{p}^{\pm}\Big)\,.\end{aligned} \tag{2}$$

Eliminating $\mathbf{IR}^{p_1}$. The function $\mathrm{IR}_K^{p_1}$ is called a total amount of $2q$ times: q times for $\mathrm{IV} = \mathrm{IV}_{\mathrm{KE}}$ with a requested output of $n-k$ bits, and q times for $\mathrm{IV} = \mathrm{IV}_{\mathrm{A}}$ with a requested output of k bits. It is a duplex construction, and we can rely on the leakage resilience of the duplex. The following Proposition 4 is very similar to [7, Corollary 1]: it is based on slightly different parametrization, but we have performed the same simplifications on the bound.

Proposition 4. *Assume that $4 \leq k \leq n$, and $1 \leq \lambda \leq 2n$. Let $p_1 \xleftarrow{\$} \mathsf{perm}(n)$ and $K \xleftarrow{\$} \{0,1\}^k$. Let $\mathsf{AIXIF1}^{ro}$ be an idealized duplex function based on a random oracle (details can be found in [7]). Let $\mathcal{L} = \{L : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^\lambda\}$ be a class of leakage functions.*

For any adversary $\mathcal{A}'$ making $q \geq 2$ queries for IV_{KE} and $q \geq 2$ queries for IV_{KA}, all of length at most k bits, and P primitive queries to p_1,

$$\begin{aligned}\mathbf{Adv}^{\text{nalr-duplex}}_{\mathrm{IR}}(\mathcal{A}') &= \max_{L\in\mathcal{L}} \Delta_{\mathcal{A}'}\left([\mathrm{IR}_K^{p_1}]_L, p_1^{\pm}\ ;\ [\mathsf{AIXIF1}_K^{ro}]_L, p_1^{\pm}\right)\\ &\leq \frac{8kqP + 4k^2q^2}{2^{n-4\lambda}} + \frac{\binom{4+2kq+P}{2} + \binom{P}{2}}{2^n} + \frac{2P}{2^{k-2\lambda}} + \frac{1}{2^k}\,. \end{aligned} \tag{3}$$

In addition, except with probability at most the same bound, all output states after absorption have min-entropy at least $n - \lambda$.

A simple hybrid reduction allows us to replace $\mathrm{IR}_K^{p_1}$ by $\mathsf{AIXIF1}_K^{ro}$ in (2):

$$\begin{aligned}(2) &\leq \Delta_{\mathcal{A}}\Big(\Big[\mathcal{E}^{\mathsf{AIXIF1}_K^{ro},\mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}\Big]_L, \Big[\mathcal{D}^{\mathsf{AIXIF1}_K^{ro},\mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}\Big]_L,\\ &\qquad \mathcal{E}^{\mathsf{AIXIF1}_K^{ro},\mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}, \mathcal{D}^{\mathsf{AIXIF1}_K^{ro},\mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}, \boldsymbol{p}^{\pm}\ ;\\ &\qquad \Big[\mathcal{E}^{\mathsf{AIXIF1}_K^{ro},\mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}\Big]_L, \Big[\mathcal{D}^{\mathsf{AIXIF1}_K^{ro},\mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}\Big]_L, \$_{*+k}, \bot, \boldsymbol{p}^{\pm}\Big)\\ &\quad + 2\cdot\Delta_{\mathcal{A}'}\left([\mathrm{IR}_K^{p_1}]_L, p_1^{\pm}\ ;\ [\mathsf{AIXIF1}_K^{ro}]_L, p_1^{\pm}\right)\\ &\leq \Delta_{\mathcal{A}}\Big(\Big[\mathcal{E}^{\mathsf{AIXIF1}_K^{ro},\mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}\Big]_L, \Big[\mathcal{D}^{\mathsf{AIXIF1}_K^{ro},\mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}\Big]_L,\\ &\qquad \mathcal{E}^{\mathsf{AIXIF1}_K^{ro},\mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}, \mathcal{D}^{\mathsf{AIXIF1}_K^{ro},\mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}, \boldsymbol{p}^{\pm}\ ;\\ &\qquad \Big[\mathcal{E}^{\mathsf{AIXIF1}_K^{ro},\mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}\Big]_L, \Big[\mathcal{D}^{\mathsf{AIXIF1}_K^{ro},\mathrm{IE}^{p_2}_{\boldsymbol{K}^\star_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}^\star_{\mathrm{KA}}}}\Big]_L, \$_{*+k}, \bot, \boldsymbol{p}^{\pm}\Big) + 2\cdot(3)\,, \end{aligned} \tag{4}$$

Towards mutually independent IE^{p_2} and IM^{p_3}. The function $\mathsf{AIXIF1}_K^{ro}$ is independent of all other functions in the oracles, and the adversary never gets its outcomes. This means that we can basically plainly replace $\boldsymbol{K}^\star_{\mathrm{KE}}$ by a dummy $\boldsymbol{K}_{\mathrm{KE}} \xleftarrow{\mathcal{D}_{\boldsymbol{K}}} (\{0,1\}^{n-k})^{2^k}$ consisting of keys with min-entropy $n-k-\lambda$. Note that $\mathsf{AIXIF1}_K^{ro}$ is called by IE^{p_2} for q different values, namely the nonces, and each nonce henceforth lets $\mathrm{IE}^{p_2}_{\boldsymbol{K}_{\mathrm{KE}}}$ select the resulting key. Likewise, we can replace $\boldsymbol{K}^\star_{\mathrm{KA}}$ by a dummy $\boldsymbol{K}_{\mathrm{KA}} \xleftarrow{\mathcal{D}_{\boldsymbol{K}}} (\{0,1\}^{k})^{2^k}$ consisting of keys with min-entropy $k-\lambda$, with the remark that identical evaluations of $\mathsf{AIXIF1}_K^{ro}$ by IM^{p_3} yield identical outputs and thus identical selections from $\boldsymbol{K}_{\mathrm{KA}}$. The step is done at the price of the bound of Proposition 4, noting that except with that bound the output states of $\mathsf{AIXIF1}_K^{ro}$ have min-entropy at least $n-k-\lambda$ resp. $k-\lambda$. Now, there is no need to keep "$\mathsf{AIXIF1}_K^{ro}$" in the equation anymore, and we obtain from (4):

$$\begin{aligned}(2) &\leq \Delta_{\mathcal{A}}\Big(\Big[\mathcal{E}^{\mathrm{IE}^{p_2}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\Big]_L, \Big[\mathcal{D}^{\mathrm{IE}^{p_2}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\Big]_L, \mathcal{E}^{\mathrm{IE}^{p_2}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}, \mathcal{D}^{\mathrm{IE}^{p_2}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}, \boldsymbol{p}^{\pm}\ ;\\ &\qquad \Big[\mathcal{E}^{\mathrm{IE}^{p_2}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\Big]_L, \Big[\mathcal{D}^{\mathrm{IE}^{p_2}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\Big]_L, \$_{*+k}, \bot, \boldsymbol{p}^{\pm}\Big)\\ &\quad + 4\cdot(3)\,. \end{aligned} \tag{5}$$

In both worlds, the encryption and authentication are mutually independent: the former is instantiated with $p_2 \xleftarrow{\$} \mathsf{perm}(n)$ and $\boldsymbol{K}_{\mathrm{KE}} \xleftarrow{\mathcal{D}_{\boldsymbol{K}}} (\{0,1\}^{n-k})^{2^k}$ and the latter is instantiated with $p_3 \xleftarrow{\$} \mathsf{perm}(n)$ and $\boldsymbol{K}_{\mathrm{KA}} \xleftarrow{\mathcal{D}_{\boldsymbol{K}}} (\{0,1\}^{k})^{2^k}$. We can therefore cleanly replace both functionalities independently.

Individual results on IE^{p_2} and IM^{p_3}. For the encryption $\mathrm{IE}^{p_2}_{\boldsymbol{K}_{\mathrm{KE}}}$, we consider it to be a duplex construction, and take a slight derivative of [7, Corollary 2], including the simplifications performed on the bound, to obtain below Proposition 5. We remark that in this derivative, we have also bounded the term q_δ, the maximum number of initialization calls for single key, probabilistically by 1. This incurred an extra term $\frac{\binom{q}{2}}{2^{n-k-2\lambda}}$. That term is, eventually, absorbed in the simplification performed on the bound.

Proposition 5. *Assume that* $4 \le k \le n$, *and* $1 \le \lambda \le 2n$. *Let* $p_2 \xleftarrow{\$} \mathsf{perm}(n)$ *and* $\boldsymbol{K}_{\mathrm{KE}} \xleftarrow{\mathcal{D}_{\boldsymbol{K}}} (\{0,1\}^{n-k})^q$ *be a random array of keys each with min-entropy at least* $n-k-\lambda$. *Let* $\mathsf{AIXIF2}^{ro}$ *be an idealized duplex function based on a random oracle (details can be found in [7]). Let* $\mathcal{L} = \{L : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^\lambda\}$ *be a class of leakage functions. For any adversary* $\mathcal{A}''$ *making* $q \ge 2$ *queries with* Q *plaintext blocks, and* $P \le 2^{n-1}$ *primitive queries to* p_2,

$$\begin{aligned}\mathbf{Adv}^{\text{nalr-duplex}}_{\mathrm{IE}}(\mathcal{A}'') &= \max_{L\in\mathcal{L}} \Delta_{\mathcal{A}''}\left(\left[\mathrm{IE}^{p_2}_{\boldsymbol{K}_{\mathrm{KE}}}\right]_L, p_2^{\pm}\ ;\ \left[\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}}\right]_L, p_2^{\pm}\right) + \frac{\binom{q}{2}}{2^{n-k-2\lambda}} \\ &\le \frac{2\mu^{Q}_{2k,n-2k}\cdot(P+1)}{2^{2k-2\lambda}} + \frac{\binom{Q}{2}}{2^{n-\lambda}} + \frac{P+qQ}{2^{n-k-2\lambda}} + \frac{\binom{Q+P}{2}+\binom{P}{2}}{2^n}\,. \end{aligned} \tag{6}$$

For the message authentication $\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}$, this is basically a suffix keyed sponge with properly protected key absorption function G that is $2^{-(k-\lambda)}$-uniform and $2^{-(k-\lambda)}$-universal. We obtain below Proposition 6 immediately from [8, Theorem 3].

Proposition 6. *Let* $p_3 \xleftarrow{\$} \mathsf{perm}(n)$ *and* $\boldsymbol{K}_{\mathrm{KE}} \xleftarrow{\mathcal{D}_{\boldsymbol{K}}} (\{0,1\}^k)^q$ *be a random array of keys each with min-entropy at least* $k-\lambda$. *Let* $\$_k$ *be a function that outputs random* k*-bit strings for each new arbitrarily-long input. Let* $\mathcal{L} = \{L : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^\lambda\}$ *be a class of leakage functions. For any adversary* $\mathcal{A}'''$ *making* $q \ge 2$ *queries, all of length at most* k *bits, and* $P \le 2^{n-1}$ *primitive queries to* p_3,

$$\begin{aligned}\mathbf{Adv}^{\text{nalr-prf}}_{\mathrm{IM}}(\mathcal{A}''') &= \max_{L\in\mathcal{L}} \Delta_{\mathcal{A}'''}\left(\left[\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}\right]_L, \mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}, p_3^{\pm}\ ;\ \left[\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}\right]_L, \$_k, p_3^{\pm}\right) \\ &\le \frac{2P^2}{2^{2k-1}} + \frac{\mu^{2(P-q)}_{k,n-k}}{2^{n-k}} + \frac{\mu^{2(P-q)}_{n-k,k}\cdot P}{2^{k-\lambda-\mu^{2(P-q)}_{k,n-k}\lambda}} + \frac{\mu^{2q}_{k,n-k}\cdot P}{2^{n-k-\lambda}}\,. \end{aligned} \tag{7}$$

Completing the proof. Propositions 5 and 6 allow us to advance with (5) as follows:

$$\begin{aligned}(2) \le{}& \Delta_{\mathcal{A}}\left(\left[\mathcal{E}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\right]_L, \left[\mathcal{D}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\right]_L, \mathcal{E}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}, \mathcal{D}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}, \boldsymbol{p}^{\pm}\ ;\right. \\ &\qquad \left.\left[\mathcal{E}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\right]_L, \left[\mathcal{D}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\right]_L, \$_{*+k}, \perp, \boldsymbol{p}^{\pm}\right) \\ &+ 4\cdot(3) + 2\cdot\Delta_{\mathcal{A}''}\left(\left[\mathrm{IE}^{p_2}_{\boldsymbol{K}_{\mathrm{KE}}}\right]_L, p_2^{\pm}\ ;\ \left[\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}}\right]_L, p_2^{\pm}\right) \\ \le{}& \Delta_{\mathcal{A}}\left(\left[\mathcal{E}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\right]_L, \left[\mathcal{D}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\right]_L, \mathcal{E}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}, \mathcal{D}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}, \boldsymbol{p}^{\pm}\ ;\right. \\ &\qquad \left.\left[\mathcal{E}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\right]_L, \left[\mathcal{D}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\right]_L, \$_{*+k}, \perp, \boldsymbol{p}^{\pm}\right) \\ &+ 4\cdot(3) + 2\cdot(6) \\ \le{}& \Delta_{\mathcal{A}}\left(\left[\mathcal{E}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\right]_L, \left[\mathcal{D}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\right]_L, \mathcal{E}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\$_k}, \mathcal{D}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\$_k}, \boldsymbol{p}^{\pm}\ ;\right. \\ &\qquad \left.\left[\mathcal{E}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\right]_L, \left[\mathcal{D}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\right]_L, \$_{*+k}, \perp, \boldsymbol{p}^{\pm}\right) \\ &+ 4\cdot(3) + 2\cdot(6) + 2\cdot\Delta_{\mathcal{A}'''}\left(\left[\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}\right]_L, \mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}, p_3^{\pm}\ ;\ \left[\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}\right]_L, \$_k, p_3^{\pm}\right) \\ \le{}& \Delta_{\mathcal{A}}\left(\left[\mathcal{E}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\right]_L, \left[\mathcal{D}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\right]_L, \mathcal{E}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\$_k}, \mathcal{D}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\$_k}, \boldsymbol{p}^{\pm}\ ;\right. \\ &\qquad \left.\left[\mathcal{E}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\right]_L, \left[\mathcal{D}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\mathrm{IM}^{p_3}_{\boldsymbol{K}_{\mathrm{KA}}}}\right]_L, \$_{*+k}, \perp, \boldsymbol{p}^{\pm}\right) \\ &+ 4\cdot(3) + 2\cdot(6) + 2\cdot(7)\,. \end{aligned} \tag{8}$$

The remaining distance of (8) boils down to forging a tag for $\mathcal{D}^{\mathsf{AIXIF2}^{ro}_{\boldsymbol{K}_{\mathrm{KE}}},\$_k}$, in which the adversary succeeds with probability at most $\frac{q_v}{2^k}$:

$$(2) \le 4\cdot(3) + 2\cdot(6) + 2\cdot(7) + \frac{q_v}{2^k}\,. \tag{9}$$