# From Known-Plaintext to Chosen-Ciphertext Security

Ueli Maurer and Johan Sjödin[⋆]

Department of Computer Science, ETH Zurich, CH-8092 Zurich, Switzerland
{maurer, sjoedin}@inf.ethz.ch

**Abstract.** Motivated by the quest for reducing assumptions in security proofs in cryptography, this paper is concerned with designing efficient symmetric encryption and authentication schemes based on weak pseudo-random functions (WPRF), which can be more efficiently implemented than PRFs. Damgård and Nielsen (Crypto '02) showed how to construct an efficient symmetric encryption scheme based on any WPRF that is provably secure under a chosen-*plaintext* attack. The main ingredient is a construction of a variable-output-length WPRF from any WPRF.

The results of this paper are three-fold. First, we optimize the Damgård-Nielsen encryption method by constructing a more efficient variable-output-length WPRF from any WPRF. Our construction is optimal for a large and natural class of reductions. Second, we propose an efficient construction of a PRF from any WPRF. Third, these two results imply the first efficient symmetric encryption scheme based on any WPRF that is provably secure under a chosen-*ciphertext* attack, and they also solve open questions posed by Naor and Reingold (Crypto '98) and by Damgård and Nielsen.

**Keywords:** Weak Pseudo-Random Function, Known-Plaintext Attack, Chosen-Ciphertext Attack, Symmetric Encryption

## 1 Introduction

### 1.1 Weakening of Cryptographic Assumptions

A general goal in cryptography is to prove the security of cryptographic systems under assumptions that are as weak as possible. Provably secure encryption and authentication schemes based on a *pseudo-random function* (PRF) [12] have been studied extensively [11]. Informally, a PRF is a function with a secret key that cannot be efficiently distinguished from a uniform random function even when it can be queried adaptively (this is often called a chosen-plaintext attack (CPA)).

The notion of a PRF is very strong and, indeed, it is unclear whether functions such as block ciphers proposed in the literature have this very strong security property.[1] When designing cryptographic schemes, it is prudent to postulate weaker properties as this makes it more likely that a certain function has such properties and there are potentially more efficient implementations for the weaker requirement compared to the stronger.

A very promising weaker notion of security, a *weak* PRF (WPRF), was recently proposed by Naor and Reingold [17] (see also [9]) and has already found several applications [18, 1, 9, 19]. Informally, a WPRF is a function with a secret key that cannot be efficiently distinguished from a uniform random function when given a sequence of *random* inputs and the corresponding outputs (this is often called a *known-plaintext attack* (KPA)). Highly efficient candidates for WPRFs are described in [8] (cf. [18]), although these are not targeted at this particular security notion explicitly.

[⋆] This work was partially supported by the Zurich Information Security Center. It represents the views of the authors.

[1] For example, the design criteria for AES did not include a requirement that a candidate proposal be a PRF, only that it be secure as a block cipher in certain modes of operation, against certain types of attacks.

While the design of WPRFs has not been studied as extensively as PRFs, a concrete argument showing that the WPRF notion is substantially weaker than the PRF notion is that WPRFs can have rather strong structural properties which are known to be devastating for PRFs. For instance, if $\mathcal{G}$ is a group of prime order $p$ in which the Decisional Diffie-Hellman (DDH) [10] assumption holds, then

$$F : \mathbb{Z}_p \times \mathcal{G} \to \mathcal{G} \quad \text{defined by} \quad F_k(x) := F(k,x) = x^k \tag{1}$$

is a WPRF [9] that commutes (i.e., $F_k(F_{k'}(x)) = F_{k'}(F_k(x))$). A WPRF can also be self inverse (i.e., $F_k(F_k(x)) = x$), have a small fraction of bad points (e.g. $F_k(x) = x$ or $F_k(x) = k$), and have related outputs (e.g. $F_k(x\|1) = F_k(x\|0)$ for all $x$). Such structural flaws make most encryption and authentication schemes based on PRFs completely insecure (for examples, see [9]).

In this paper we propose provably secure encryption and authentication schemes, for the strongest security notion, under the sole assumption of a WPRF. Of course, the security could also be based on even weaker assumptions like the one-wayness of a certain function, since a PRF can be obtained from any one-way function [13, 12]. However, such schemes are not of practical interest due to their inefficiency.

### 1.2 Contributions and Related Work

The main motivation for this paper is Damgård and Nielsen's elegant work on WPRFs [9]. In their paper, the Pseudorandom Tree (PRT) construction is proposed for transforming any WPRF $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ into a variable-output-length[2] (VOL) WPRF

$$\mathrm{PRT}^F : \{0,1\}^\kappa \times \{0,1\}^n \times \mathbb{N} \to \{0,1\}^*.$$

Furthermore, they show how to construct an efficient probabilistic symmetric encryption scheme from $F$ that is provably secure under a CPA[3]. This is achieved by encrypting a message $m \in \{0,1\}^*$, under a key $k \in \{0,1\}^\kappa$ and some auxiliary uniform randomness $r \in \{0,1\}^n$, as

$$(k, r, m) \mapsto \Big(r, \mathrm{PRT}_k^F(r, |m|) \oplus m\Big). \tag{2}$$

To point out the efficiency of this encryption scheme (and also as a reference for the schemes presented in this work), let us compare it with standard modes of operation such as CBC and CTR. Whereas CBC and CTR invoke the underlying block cipher once per message block to encrypt/decrypt, this scheme invokes the underlying function $F$ once per message block to encrypt/decrypt and roughly $2 \cdot \log_2(b)$ times (where $b$ is the number of message blocks) for generating more key material from the initial key (see below). The key generation can be done offline, such that the throughput is exactly the same as for CBC and CTR. However, whereas CBC and CTR are CPA-secure if the underlying block cipher is a PRF, (2) is CPA-secure even when the underlying function is a WPRF. And as WPRFs can be more efficiently implementable than PRFs, this scheme can also be the overall most efficient one. Unfortunately, these modes of operations are not secure under the stronger *chosen-ciphertext attack* (CCA)[4] notion. A natural question posed

[2] A variable output length function family $V : \{0,1\}^\kappa \times \{0,1\}^n \times \mathbb{N} \to \{0,1\}^*$ satisfies $|V_k(x,l)| = l$ for all $k, x$, and $l$.

[3] CPA security (for an encryption scheme) formalizes an adversary's inability, given access to an encryption oracle, to distinguish between two plaintexts given the encryption of one of them.

[4] In a CCA attack the adversary also has access to a decryption oracle.

by Naor and Reingold [17, p. 279] and by Damgård and Nielsen [9, p. 464] (which also is the main motivation for this paper) is whether such schemes can be constructed efficiently from any WPRF.

Before we present our results, let us briefly describe the underlying idea of the PRT-construction (illustrated in Fig. 1(c) on page 8). In a first step, some key material $k_0, \ldots, k_j$ is generated from the initial key $k$ by invoking $F$ in an iterative manner, and then the output blocks are derived by applying $F_{k_i}$, for some $i \in \{0, \ldots, j\}$, iteratively to the input or a previously derived output block. For constructions of this type it is crucial for the security and the efficiency (in terms of the number of applications of $F$ relative to the output length) that this is scheduled in the right way. Recently, two more efficient VOL-WPRF constructions of this type, the Expanded PRT (ERT) (see Fig. 1(b)) and the Factorial Tree (FCT), were proposed in [16]. However, as shown in Sect. 3.2, the latter and more efficient construction of the two turns out to be insecure. A natural question that arises is whether a more efficient (or even the most efficient) construction can be found.

The contributions of this paper are the following:

1. The Increasing Chain Tree (ICT) construction – An optimal VOL-WPRF from any WPRF:
Our ICT- construction (see Fig. 1(a)) is more efficient and uses a shorter initial key than the previous constructions PRT and ERT. Interestingly, the generated key sequence $k_0, \ldots, k_j$ is not pseudorandom as opposed to the case for PRT and ERT. Indeed, we show that ICT is optimal for the large and natural class of constructions described above. This result implies an optimization of the CPA-secure encryption scheme described in (2) by replacing PRT by ICT.
2. The Increasing Chain (IC) construction – A construction of a PRF from any WPRF:
Our IC-construction is similar in nature to Goldreich, Goldwasser, and Micali's (GGM) [12] construction of a PRF from any PRG, but it is more than twice as efficient than first transforming the WPRF into a PRG and then applying the GGM-construction. It is also more efficient than Naor and Reingold's construction of a PRF based on any WPRF [18][5]. This solves their open problem [17, p. 278] whether a more efficient construction exist positively.
In particular, if we instantiate the IC-construction with the DDH-based WPRF $F$ defined in (1), we get Naor and Reingold's construction [19] of a PRF based on the DDH assumption but with a non-trivial[6] reduction of the key-material by a factor of roughly the input length of the PRF.
3. A CCA-secure encryption scheme from any WPRF:
Results 1 and 2, combined with a Wegman-Carter [22] based message authentication code (MAC) and the well-known encrypt-then-MAC method [15, 6], yield the first efficient encryption scheme from any WPRF that is secure under a CCA and hence settles the open question mentioned above. We observe that for our purpose a much weaker primitive than the MAC, namely a *weak* MAC (WMAC)[7], is sufficient, i.e., encrypt-then-WMAC actually does the job.
4. A non-adaptive[8] CCA-secure encryption scheme from any WPRF and WMAC:
This type of security may (as CPA-security) be unsatisfactory in practice, but the exact requirements for achieving standard security notions are interesting in their own right. It might also motivate further research on basing strong primitives on weak assumptions. Non-adaptive CCA-security has been studied under stronger assumptions in [17].

[5] In this work the PRF is reduced to a pseudo-random synthesizer, which in turn is reduced to a WPRF.

[6] By non-trivial we mean that the key is not replaced by a pseudorandom sequence based on $F$.

[7] A WMAC is also referred to as a MAC which is secure (or unforgeable) under a *known-plaintext attack* (see [17]).

[8] Here the adversary does not have access to the oracles after the challenge (ciphertext) is presented.

## 2 Preliminaries

### 2.1 Notation and Definitions

Let $s \overset{\$}{\leftarrow} S$ denote the operation of selecting $s$ uniformly at random from the set $S$. If $\mathcal{D}$ is a probability distributions over $S$ then $s \leftarrow \mathcal{D}$ denotes the operation of selecting $s$ at random according to $\mathcal{D}$. Let $\mathcal{U}_n$ denote the uniform distribution over $\{0,1\}^n$. Furthermore, $\mathcal{R}_{L,\ell}$ and $\mathcal{R}_{\leq L,\ell}$ denote random functions with range $\{0,1\}^\ell$, and domain $\{0,1\}^L$ and $\{0,1\}^{\leq L} := \cup_{i=1}^{L}\{0,1\}^i$, respectively. For two functions $f$ and $g$, let $f \circ g\,(x) := f(g(x))$. If $x$ and $y$ are two bitstrings, $x\|y$ denotes their concatenation, $x[i]$ the $i^{th}$ bit of $x$, and $x[i,j] := x[i]\|x[i+1]\|\cdots\|x[j]$ with $i < j$. $A^{\mathcal{O}}$ denotes an algorithm $A$ with oracle access to $\mathcal{O}$. $\Pr[\mathit{\Pi} : \mathcal{E}]$ is the probability that event $\mathcal{E}$ occurs in random experiment $\mathit{\Pi}$.

### 2.2 Cryptographic Functions

We state our results in the concrete security framework introduced by Bellare, Kilian, and Rogaway [5] and which has been used in many subsequent works [3, 4, 6]. Let $\mathcal{O}^f$ denote an oracle which, if invoked, returns $(r, f(r))$, where $f$ is a function and $r$ a uniformly at random chosen input of $f$. Let $F : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^\ell$ be a function family and $g : \{0,1\}^\kappa \to \{0,1\}^n$ a function (with $\kappa < n$). The $\mathbf{w}$-*advantage* of adversary $A$, for $\mathbf{w} \in \{\mathbf{prf}, \mathbf{wprf}, \mathbf{mac}, \mathbf{wmac}, \mathbf{prg}\}$, is defined as

$$\begin{aligned}
\mathbf{Adv}^{\mathbf{prf}}_{F,A} &:= \Pr\big[k \leftarrow \mathcal{U}_\kappa, b \leftarrow A^{F_k} : b = 1\big] - \Pr\big[R \leftarrow \mathcal{R}_{n,\ell}, b \leftarrow A^R : b = 1\big] \\
\mathbf{Adv}^{\mathbf{wprf}}_{F,A} &:= \Pr\Big[k \leftarrow \mathcal{U}_\kappa, b \leftarrow A^{\mathcal{O}^{F_k}} : b = 1\Big] - \Pr\Big[R \leftarrow \mathcal{R}_{n,\ell}, b \leftarrow A^{\mathcal{O}^R} : b = 1\Big] \\
\mathbf{Adv}^{\mathbf{mac}}_{F,A} &:= \Pr\left[k \leftarrow \mathcal{U}_\kappa, (m,\tau) \leftarrow A^{F_k}, b = \begin{cases} 1 & \text{if } \tau = F_k(m),\ m \text{ ``new''} \\ 0 & \text{otherwise} \end{cases} : b = 1\right] \\
\mathbf{Adv}^{\mathbf{wmac}}_{F,A} &:= \Pr\left[k \leftarrow \mathcal{U}_\kappa, (m,\tau) \leftarrow A^{\mathcal{O}^{F_k}}, b = \begin{cases} 1 & \text{if } \tau = F_k(m),\ m \text{ ``new''} \\ 0 & \text{otherwise} \end{cases} : b = 1\right] \\
\mathbf{Adv}^{\mathbf{prg}}_{g,A} &:= \Pr[k \leftarrow \mathcal{U}_\kappa, b \leftarrow A(g(k)) : b = 1] - \Pr[r \leftarrow \mathcal{U}_n, b \leftarrow A(r) : b = 1]
\end{aligned}$$

and the corresponding maximal advantages as

$$\mathbf{Adv}^{\mathbf{w}}_{F}(t,q) := \max_A\{\mathbf{Adv}^{\mathbf{w}}_{F,A}\} \quad \text{and} \quad \mathbf{Adv}^{\mathbf{prg}}_{g}(t) := \max_A\{\mathbf{Adv}^{\mathbf{prg}}_{g,A}\},$$

where the maximum is taken over all $A$ restricted to $q$ (respectively $q-1$ in case of the **mac** or **wmac** notion) invocations of its oracle and the standard time-complexity $t$.[9]

Next, we describe both the notion of a variable-input-length (VIL) function family and a variable-output-length (VOL) function family.

[9] I.e., we distinguish between the case when the advantage of an adversary $A$ is a difference between the probability that an event (i.e., $b = 1$ in the above cases) occurs in two different random experiments and the case when the advantage is simply the probability that an event occurs in a single experiment. In the former case, $t$ is the maximum of the worst-case total running time of the different experiments, and in the latter case, $t$ is the worst-case total running time of the experiment (in some fixed RAM model of computation). We also adopt the convention that $t$ includes the length of the RAM program describing $A$.

**Definition 1.** *A function family* $F : \{0,1\}^\kappa \times \{0,1\}^{\leq N} \to \{0,1\}^n$ *is referred to as having* variable-input-length *(VIL).*

The **vil-mac**-advantage $\mathbf{Adv}^{\textbf{vil-mac}}_{F,A}$ is defined as $\mathbf{Adv}^{\textbf{mac}}_{F,A}$ except that the adversary may query its oracle with inputs of any length ($\leq N$), and the **vil-wmac**-advantage $\mathbf{Adv}^{\textbf{vil-wmac}}_{F,A}$ is defined as $\mathbf{Adv}^{\textbf{wmac}}_{F,A}$ except that the oracle $\mathcal{O}^{F_k}$ is replaced by an oracle $\mathcal{O}^{F_k}_{\textbf{vil}}$ that on input $l \leq N$ outputs $(r, F_k(r))$ where $r \xleftarrow{\$} \{0,1\}^l$. The maximal **vil-mac**- and **vil-wmac**-advantage is defined as

$$\mathbf{Adv}^{\textbf{vil-mac}}_{F}(t,q,\mu) := \max_A\{\mathbf{Adv}^{\textbf{vil-mac}}_{F,A}\} \quad \text{and}$$
$$\mathbf{Adv}^{\textbf{vil-wmac}}_{F}(t,q,\mu) := \max_A\{\mathbf{Adv}^{\textbf{vil-wmac}}_{F,A}\},$$

respectively, where the maximum is taken over all $A$ restricted to time-complexity $t$ and at most $q-1$ oracle invocations for which the total length of the inputs to $F$ is at most $\mu$ bits including the forgery message.

**Definition 2.** *A function family* $F : \{0,1\}^\kappa \times \{0,1\}^n \times \mathbb{N} \to \{0,1\}^*$ *is referred to as having* variable-output-length *(VOL) if* $|F_k(x,l)| = l$*, for all* $k$*,* $x$*, and* $l$*.*

The security notion of a VIL-WPRF is defined as follows [9]. Let $\mathcal{R}_{n,*}$ denote the following probabilistic function. On input $(x,l)$ check whether a string $o_x$ is defined; if not define it to be the empty string. Then check whether $o_x$ has length at least $l$; if not append to $o_x$ a uniformly at random chosen string from $\{0,1\}^{l-|o_x|}$. Then output $o_x[1,l]$. Let $\mathcal{O}^f_{\textbf{vol}}$ be an oracle that on input $l$ outputs $(x, f(x,l))$ for uniformly at random chosen $x$. The **vol-wprf**-advantage of adversary $A$ in attacking $F$ is

$$\mathbf{Adv}^{\textbf{vol-wprf}}_{F,A} := \Pr\Big[k \leftarrow \mathcal{U}_\kappa, b \leftarrow A^{\mathcal{O}^{F_k}_{\textbf{vol}}} : b=1\Big] - \Pr\Big[k \leftarrow \mathcal{U}_\kappa, b \leftarrow A^{\mathcal{O}^{\mathcal{R}_{n,*}}_{\textbf{vol}}} : b=1\Big]$$

and the maximal **vol-wprf**-advantage as

$$\mathbf{Adv}^{\textbf{vol-wprf}}_{F}(t,q,\mu) := \max_A\{\mathbf{Adv}^{\textbf{vol-wprf}}_{F,A}\},$$

where the maximum is taken over all $A$ restricted to time-complexity $t$ and at most $q$ samples for which the output lengths of $F$ total at most $\mu$ bits.

## 3 The IC and ICT Constructions

In this section we introduce the IC-construction, for transforming a WPRF into a PRF, and the ICT-construction, for transforming a WPRF into a VOL-WPRF. Throughout this section, let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a function family and $t_F$ the worst-case running time for computing $F$.

### 3.1 A PRF from any WPRF

The IC-construction transforms $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ into

$$\mathrm{IC}^F : (\{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n) \times \{0,1\}^N \to \{0,1\}^n,$$

for some fixed $N$, and is defined by the following algorithm for computing $\mathrm{IC}^F_{k_0,r,\tau_0}(x)$:

```
for $i = 1$ to $|x|-1$ do
   $k_i = F_{k_{i-1}}(r)$
for $i = 1$ to $|x|$ do
   if $x[i] = 1$ then
      $\tau_i = F_{k_{i-1}}(\tau_{i-1})$
   else
      $\tau_i = \tau_{i-1}$
return $\tau_{|x|}$
```

The following theorem states that $\mathrm{IC}^F$ is a PRF if $F$ is a WPRF. The proof is given in Appendix A.[10] Note that $F$ is invoked at most $2N-1$ times. However, the first $N-1$ invocations can be pre-processed and cached, and hence at most $N$ invocations are necessary or, to be precise, as many invocations as there are ones in the input.

**Theorem 1.** *For any $t$, $q$, and input length $N$ of* $\mathrm{IC}^F$

$$\mathbf{Adv}^{\mathbf{prf}}_{\mathrm{IC}^F}(t,q) \leq N \cdot \left( \mathbf{Adv}^{\mathbf{wprf}}_{F}(t,q) + \frac{q(q+1)}{2^{n+1}} \right).$$

*Reducing the key material of Naor-Reingold's PRF based on the DDH assumption.* In [19], Naor and Reingold presented an efficient construction of a PRF based on the DDH assumption. It is easy to verify, that $\mathrm{IC}^F$ with $F$ as defined in (1) is the same construction but with a significantly shorter key by a factor of roughly $N$ (recall that $N$ is the input length of $\mathrm{IC}^F$). To be more precise, the first for-loop (in the IC-algorithm) generates a sequence $k_0, \ldots, k_{N-1}$ of keys from the initial key $(k_0, r, \tau_0)$ and the second for-loop exactly corresponds to the Naor-Reingold construction with $k_0, \ldots, k_{N-1}$ as its key. The reduction is non-trivial in the sense that $k_0, \ldots, k_{N-1}$ is not generated from a PRG based on $F$. For instance $F^{-1}_{k_1}(k_2) = F^{-1}_{k_2}(k_3)$ holds which can easily be verified given $k_1, k_2, k_3$.

Furthermore, it can be shown that the $r$-value (of the initial key) need not be kept secret.

*Comparisons to the GGM-construction [12].* A PRF can also be constructed by first transforming the WPRF $F$ into a length doubling PRG and then applying the GGM-construction. To illustrate that IC is the more efficient construction, let us briefly describe the GGM construction. It transforms a length doubling PRG $G$ (say from $n$ to $2n$ bits) into a PRF (say from $N$ to $n$ bits) as follows:

$$GGM_k(x_1 \| \ldots \| x_N) := G_{x_1} \circ \ldots \circ G_{x_N}(k),$$

where the $x_i$'s are bits, and $G_0(k)$ and $G_1(k)$ denote the left and right half of $G(k)$, respectively. To our knowledge, the best construction of a length doubling PRG $G$ from $F$ uses 6 invocations of $F$ per call to $G$ (see Remark 5 in Appendix B), and for computing $G_0$ and $G_1$ separately one needs 3 and 4 invocations to $F$, respectively. To get a PRF with $N$-bits input and $n$-bits output, we hence need roughly $4N$ invocations of $F$ per call in the worst case (cf. the efficiency of $\mathrm{IC}^F$).

[10] We refer to [9] for constructing an $n$-bit block WPRF $F$ from any WPRF.

### 3.2 A VOL-WPRF from any WPRF

The ICT-construction is illustrated in Fig. 1(a) and is defined as

$$\begin{aligned} \mathrm{ICT}^F : \{0,1\}^{2n} \times \{0,1\}^n \times \mathbb{N} &\to \{0,1\}^* \\ (k\|r, x, l) &\mapsto \left(\mathrm{IC}^F_{k,r,x}(\langle 1\rangle)\| \cdots \| \mathrm{IC}^F_{k,r,x}(\langle \lceil l/n \rceil\rangle)\right)[1,l], \end{aligned}$$

where $\langle i\rangle$ denotes the standard bit encoding of the integer $i$. The next theorem states that $\mathrm{ICT}^F$ is a VOL-WPRF if $F$ is a WPRF. It is easy to verify that for computing $\mathrm{ICT}^F(k\|r, x, l)$, we need $d = \lfloor \log_2(\lceil l/n \rceil)\rfloor$ calls to $F$ for computing (or pre-computing) the needed keys $k_0, \ldots, k_d$ (cf. Fig. 1(a)) and further $\lceil l/n\rceil$ calls for computing the output (i.e., one call per output block).

**Theorem 2.** *For any $t, q$, and $\mu$*

$$\mathbf{Adv}^{\textbf{vol-wprf}}_{\mathrm{ICT}^F}(t,q,\mu) \le d_{\max} \cdot \mathbf{Adv}^{\textbf{wprf}}_{F}(t', q2^{d_{\max}-1}+1) + \frac{4^{d_{\max}} \cdot q^2 - q}{2^{n+1}},$$

*where $t' = t + \mathcal{O}(\frac{q \cdot l_{\max}}{n} \cdot t_F)$, $d_{\max} = \lfloor \log_2(\lceil l_{\max}/n\rceil)\rfloor + 1$, and $l_{\max} \le \mu$ is the maximum allowed output length of* $\mathrm{ICT}^F$.

The proof is provided in Appendix B. It can further be shown that the second half of the key, namely the $r$-value, need not be kept secret.

*The FCT-construction is flawed.* Let us point out that the security proof of the FCT-construction (in [16]) is flawed. Moreover, since (for instance) the maximal sized output of $\mathrm{FCT}^F$ for two generated keys $k_0, k_1$ is defined as

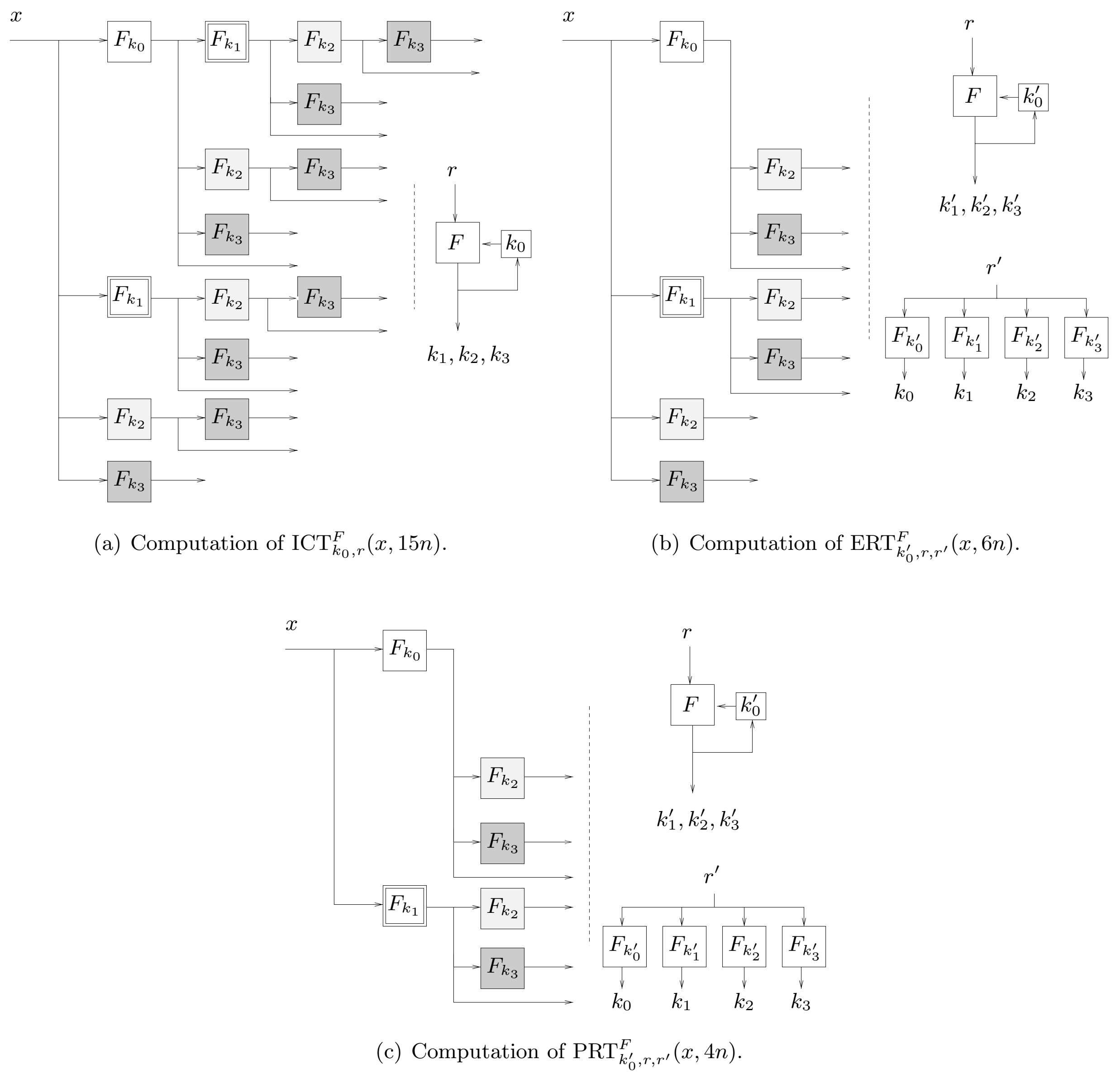
$$x \mapsto F_{k_0}(x)\|F_{k_1}(x)\|F_{k_0} \circ F_{k_1}(x)\|F_{k_1} \circ F_{k_0}(x),$$

the construction is insecure for WPRFs $F$ that commute (i.e., for which $F_k \circ F_{k'}(x) = F_{k'} \circ F_k(x)$ for all $k$, $k'$, $x$). Since such WPRFs exist under the DDH assumption (see (1)), a fix of the security proof would contradict the assumption and thus be a major breakthrough in number theory.

*Comparing* ICT *with other constructions.* The idea behind PRT of [9], ERT of [16], and ICT is to first generate keys $k_0, \ldots, k_d$ from the initial key (and $F$) and then to derive the output blocks sequentially by invoking $F_{k_i}$ (with $i \in \{0, \ldots, d\}$) to the input or a previously computed output block (see Fig. 1).

ICT is superior to PRT and ERT for three reasons. First, the initial key of ICT is $n$ bits (plus $n$ bits that may be publicly known) versus $3n$ bits for PRT and ERT. Second, ICT needs $d$ invocations of $F$ to generate the keys $k_0, \ldots, k_d$ whereas PRT and ERT needs $2d + 1$. Third, the maximal output size using $k_0, \ldots, k_d$ is $(2^{d+1}-1)n$ for ICT, roughly $(3^{\frac{d+1}{2}}-1)n$ for ERT, and roughly $(2^{\frac{d+1}{2}+1}-2)n$ for PRT.[11] Allowing pre-processing of the keys, all these constructions need one call of $F$ per output block, but whereas ICT needs to store say $s$ keys, ERT and PRT needs to store about $\lceil 1.26 \cdot s\rceil$ and $2 \cdot s$ keys, respectively (for the same maximal output length). As we show next ICT is actually optimal (for constructions of this nature).

[11] The latter two values are exact if $d$ is odd. Otherwise $(2 \cdot 3^{\frac{d}{2}} - 1)n$ and $(3 \cdot 2^{\frac{d}{2}} - 2)n$ are exact, respectively.



(a) Computation of $\mathrm{ICT}^F_{k_0,r}(x, 15n)$.

(b) Computation of $\mathrm{ERT}^F_{k'_0,r,r'}(x, 6n)$.

(c) Computation of $\mathrm{PRT}^F_{k'_0,r,r'}(x, 4n)$.

**Fig. 1.** The following figure illustrates, (a) the ICT-construction of this paper, (b) the ERT-construction of [16], and (c) the PRT-construction of [9]. Each figure corresponds to the computation of the output of maximal size using 4 (generated) keys. The key generation is illustrated to the right of the dashed line in each figure. Interestingly, the generated key sequence, i.e., $k_0, \ldots, k_3$, is not pseudo-random in (a) as opposed to in (b) and (c) (cf. Sect. 3.1).

*The ICT-construction is optimal.* The value $\mathrm{ICT}^F_{k_0,r}(x,l)$, where $l = 3n$, is computed by first computing $k_1 = F_{k_0}(r)$ and then returning

$$y := F_{k_0}(x) \| F_{k_1}(x) \| F_{k_1} \circ F_{k_0}(x).$$

For $l = 7n$, an extra key $k_2 = F_{k_1}(r)$ is derived and then the following is returned

$$y \| F_{k_2}(x) \| F_{k_2} \circ F_{k_0}(x) \| F_{k_2} \circ F_{k_1}(x) \| F_{k_2} \circ F_{k_1} \circ F_{k_0}(x).$$

Note that for each $n$-bit output block, the key indices in the evaluations of $F$ occur in increasing order. A natural question is whether more can be output before a new key needs to be generated, i.e., can we using *one* extra call to $F$ output more than $\mathrm{ICT}^F$ maximally can for a fixed number of generated keys. The answer turns out to be "no" unless the Inverse Decisional Diffie Hellman (IDDH) assumption [2] is false, since (under this assumption) there is a WPRF $F$, described in (3) below, which with high probability both commutes, i.e., $\Pr_{k,k',x}[F_k \circ F_{k'}(x) = F_{k'} \circ F_k(x)] \approx \frac{1}{4}$, and is self inverse, i.e., $\Pr_{k,x}[F_k \circ F_k(x) = x] \approx \frac{1}{2}$. If $F$ is used and more is output at least two output blocks will have the same value with high probability (which is unlikely the case for $\mathcal{R}_{n,*}$). As a consequence ICT is optimal for constructions of this type. The function $F$ is defined as follows:

$$F : \mathbb{Z}_p \times \mathcal{G} \to \mathcal{G} \quad \text{and} \quad F_k(x) := \begin{cases} x^k & \text{if } x \in P_1 \\ x^{k^{-1}} & \text{if } x \in P_2 \end{cases}, \tag{3}$$

where $\mathcal{G}$ is a group of prime order $p$, $k^{-1}$ satisfies $k \cdot k^{-1} = 1 \pmod p$, and $P_1$, $P_2$ is a partition of $\mathcal{G}$ in roughly equal sized sets.[12] The proof that $F$ is a WPRF if the IDDH assumption holds in $\mathcal{G}$ can easily be derived using results from [2].

## 4 Applications

By applying our results, we optimize Damgård and Nielsen's CPA-secure encryption scheme (see (2)), and propose new methods for achieving non-adaptive and adaptive CCA-security efficiently.

### 4.1 Symmetric Encryption

A symmetric encryption scheme $\mathcal{SE} = (E, D)$ consists of two efficient algorithms. The (randomized) encryption algorithm $E$ maps a key $k$ and a message $m$ to a ciphertext $c = E_k(m)$, and the deterministic decryption algorithm $D$ maps a key $k$ and a ciphertext $c = E_k(m)$ to the message $m = D_k(c)$. There are several notions for privacy and integrity of $\mathcal{SE}$ (for an overview, we refer to [6, 14, 3]).

We consider the privacy notion IND-PX-CY for X,Y $\in \{0,1,2\}$ as introduced in [14]. The following is a concrete version of their definition:

**Definition 3 (IND-PX-CY).** *Let $\mathcal{M}$ and $\mathcal{K}$ denote the message- and key-space, respectively, of $\mathcal{SE} = (E, D)$. The* **ind-p***$x$***-c***$y$-advantage of an adversary $A$ for $\mathcal{SE}$ and $x, y \in \{0,1,2\}$ is defined as follows (where $\perp$ denotes no oracle).*

[12] In addition it must be efficient to decide whether $x \in P_1$ (or not).

$$\mathbf{Adv}^{\textbf{ind-p}x\textbf{-c}y}_{\mathcal{SE},A} := 2\cdot\Pr\Big[k \xleftarrow{\$} \mathcal{K}, (m_0,m_1) \leftarrow A^{\mathcal{O}_1,\mathcal{O}_2}, b \xleftarrow{\$} \{0,1\}, c \leftarrow E_k(m_b), \hat{b} \leftarrow A^{\mathcal{O}'_1,\mathcal{O}'_2}(c) : \hat{b} = b\Big] - 1,$$

*where* $(\mathcal{O}_1, \mathcal{O}'_1) = \begin{cases} (\perp,\perp) & \textit{if } x = 0 \\ (E_k,\perp) & \textit{if } x = 1 \\ (E_k,E_k) & \textit{if } x = 2 \end{cases}$, $(\mathcal{O}_2, \mathcal{O}'_2) = \begin{cases} (\perp,\perp) & \textit{if } y = 0 \\ (D_k,\perp) & \textit{if } y = 1 \\ (D_k,D_k) & \textit{if } y = 2 \end{cases}$,

$m_0, m_1 \in \mathcal{M}$ *with* $|m_0| = |m_1|$, *and* $A$ *does not query* $\mathcal{O}'_2$ *with* $c$. *Furthermore, let*

$$\mathbf{Adv}^{\textbf{ind-p}x\textbf{-c}y}_{\mathcal{SE}}(t,q,\mu,q',\mu') := \max_A\{\mathbf{Adv}^{\textbf{ind-p}x\textbf{-c}y}_{\mathcal{SE},A}\},$$

*where the maximum is taken over all* $A$ *restricted to time-complexity* $t$, *at most* $q-1$ *encryption queries of total length at most* $(\mu - |m_0|)$ *bits, and* $q'$ *decryption queries of total length at most* $\mu'$ *bits.*[13]

The IND-P2-C0, IND-P1-C1, and IND-P2-C2 notions are often referred to as IND-CPA, non-adaptive IND-CCA, and (adaptive) IND-CCA, respectively.[14]

The strongest integrity notion for encryption schemes is *integrity of ciphertexts* (INT-CTXT) [6]:

**Definition 4 (INT-CTXT).** [6] *Let* $\mathcal{K}$ *denote the key space of* $\mathcal{SE} = (E, D)$ *and* $D^*_k$ *an algorithm that on input* $c$ *outputs* $1$ *iff* $c$ *is a valid ciphertext under the key* $k$. *Furthermore, let* $x_1, \ldots, x_q$ *and* $y_1, \ldots, y_{q'}$ *denote adversary* $A$*'s oracle queries to* $E_k$ *and* $D^*_k$, *respectively. Then*

$$\mathbf{Adv}^{\textbf{int-ctxt}}_{\mathcal{SE},A} := \Pr\left[k \xleftarrow{\$} \mathcal{K}, A^{E_k,D^*_k}, b := \begin{cases} 1 & \textit{If } \exists i\ \forall j : D^*_k(y_i) = 1 \wedge y_i \neq E_k(x_j) \\ 0 & \textit{otherwise} \end{cases} : b = 1\right]$$

*and* $\mathbf{Adv}^{\textbf{int-ctxt}}_{\mathcal{SE}}(t,q,\mu,q',\mu') := \max_A\{\mathbf{Adv}^{\textbf{int-ctxt}}_{\mathcal{SE},A}\}$ *for all* $t$, $q$, $\mu$, $q'$, *and* $\mu'$, *where the maximum is taken over all* $A$ *restricted to time-complexity* $t$, *at most* $q$ *queries to* $E_k$ *of total length at most* $\mu$ *bits, and at most* $q'$ *queries to* $D^*_k$ *of total length at most* $\mu'$ *bits.*

### 4.2 A CPA-Secure Encryption Scheme

Damgård and Nielsen [9] introduced the following mode of operation for constructing a IND-P2-C0 secure encryption scheme based on any VOL-WPRF $V : \{0,1\}^\kappa \times \{0,1\}^n \times \mathbb{N} \to \{0,1\}^n$. Let $\mathcal{SE}_1$ denote the symmetric encryption scheme defined by encrypting a message $m \in \{0,1\}^*$, under the key $k \in \{0,1\}^\kappa$ and some auxiliary uniform randomness $r \in \{0,1\}^n$, as

$$(k, r, m) \mapsto \Big(r, V_k(r, |m|) \oplus m\Big). \qquad (\mathcal{SE}_1) \qquad (4)$$

The following proposition, similarly given in [9], states that $\mathcal{SE}_1$ is IND-P2-C0-secure if $V$ is a VOL-WPRF. For completeness, the proof is provided in Appendix C.

**Proposition 1.** *For any* $t, q,$ *and* $\mu$

$$\mathbf{Adv}^{\textbf{ind-p2-c0}}_{\mathcal{SE}_1}(t,q,\mu) \leq 2 \cdot \mathbf{Adv}^{\textbf{vol-wprf}}_{V}(t,q,\mu) + \frac{q-1}{2^{n-1}}.$$

[13] The parameters $(q, \mu)$ and $(q', \mu')$ are omitted when $x = 0$ and $y = 0$, respectively.

[14] As shown in [14], IND-P1-CY implies IND-P2-CY for $\mathsf{Y} \in \{0,1,2\}$. Furthermore, IND-P2-C0 and IND-P2-C2 are equivalent to FTG-CPA and FTG-CCA, respectively, and FTG implies the ROR, LOR, and SEM notions [3].

We optimize the above scheme by using ICT as VOL-WPRF (as opposed to PRT, cf. (2)), i.e.,

$$(k, r, m) \mapsto \Big(r, \mathrm{ICT}_k(r, |m|) \oplus m\Big). \qquad (\mathcal{SE}'_1) \qquad (5)$$

The security proof follows directly from Proposition 1 and Theorem 2.

**Corollary 1.** *For any $t, q$ and $\mu$,*

$$\mathbf{Adv}^{\textbf{ind-p2-c0}}_{\mathcal{SE}'_1}(t, q, \mu) \leq 2 \cdot d_{\max} \cdot \mathbf{Adv}^{\textbf{wprf}}_{F}(t', q2^{d_{\max}-1}) + \frac{4^{d_{\max}} \cdot q^2 + q}{2^n},$$

*where $t' = t + \mathcal{O}(\frac{q \cdot l_{\max}}{n} \cdot t_F)$, $d_{\max} := \lfloor \log_2(\lceil l_{\max}/n \rceil) \rfloor + 1$, and $l_{\max} \leq \mu$ is the maximum allowed output length of* $\mathrm{ICT}^F$.

*Remark 1.* As for the encryption scheme defined by using PRT as VOL-WPRF in (4), this mode of operation (using ICT as VOL-WPRF instead) needs one invocation of $F$ per message block to encrypt/decrypt[15] as the generated keys that are used can be pre-processed (if no pre-processing is used ICT is more efficient, cf. Section 3.2). The main advantage of using ICT instead of PRT is not only that a shorter initial key is needed, the number of generated keys which need to be securely stored (in case of the pre-processing) is also reduced by a factor of roughly 2. Given the strong optimality arguments for ICT it appears as this is the best possible for this mode of operation.

### 4.3 A Non-Adaptive CCA-Secure Encryption Scheme

To achieve IND-P2-C1-security of $\mathcal{SE}_1$ we note that it is sufficient to WMAC the auxiliary randomness $r$. To be precise, for $V : \{0,1\}^{\kappa_1} \times \{0,1\}^n \times \mathbb{N} \to \{0,1\}^*$ and $W : \{0,1\}^{\kappa_2} \times \{0,1\}^n \to \{0,1\}^\ell$ let $\mathcal{SE}_2$ denote the encryption scheme defined by encrypting a message $m \in \{0,1\}^*$ under the key $(k_1, k_2) \in \{0,1\}^{\kappa_1} \times \{0,1\}^{\kappa_2}$ and some auxiliary uniform randomness $r \in \{0,1\}^n$ as

$$(k_1, k_2, r, m) \mapsto \Big(r, V_{k_1}(r, |m|) \oplus m, W_{k_2}(r)\Big). \qquad (\mathcal{SE}_2) \qquad (6)$$

The following theorem states that $\mathcal{SE}_2$ is IND-P2-C1-secure if $V$ is a VOL-WPRF and $W$ is a WMAC. The proof is provided in Appendix C.

**Theorem 3.** *For any $t, q, \mu, q'$, and $\mu'$*

$$\mathbf{Adv}^{\textbf{ind-p2-c0}}_{\mathcal{SE}_2}(t, q, \mu) \leq \mathbf{Adv}^{\textbf{ind-p2-c0}}_{\mathcal{SE}_1}(t, q, \mu), \text{ and}$$

$$\mathbf{Adv}^{\textbf{ind-p2-c1}}_{\mathcal{SE}_2}(t, q, \mu, q', \mu') \leq 2 \cdot q' \cdot \mathbf{Adv}^{\textbf{wmac}}_{W}(t, q) + \mathbf{Adv}^{\textbf{ind-p2-c0}}_{\mathcal{SE}_1}(t, q, \mu).$$

*Remark 2.* Recall that if $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is a WPRF, then $\mathrm{IC}^F$ is a PRF and hence also a (W)MAC. Therefore, by for instance using $\mathrm{IC}^F$ as WMAC and $\mathrm{ICT}^F$ as VOL-WPRF in (6) results in a IND-P2-C1 secure encryption scheme from any WPRF. Since $\mathrm{IC}^F$ is invoked on random inputs, $n/2$ (or $3n/2 - 1$ in case of no pre-processing) invocations of $F$ will be needed on average for each call to $\mathrm{IC}^F$ independently of the message length.

[15] Recall that standard modes like CBC and CTR also invoke the underlying block cipher once per message block.

### 4.4 A CCA-Secure Encryption Scheme

The well-known encrypt-then-MAC method is a mode of operation for constructing an INT-CTXT- and IND-P2-C2-secure encryption scheme from any IND-P2-C0-secure encryption scheme $\mathcal{SE} = (E, D)$ and a VIL-MAC $W$. The idea is to simply encrypt with $E$ and then authenticate the ciphertext using $W$ [15, 6]. We note that for our purpose (i.e., for the IND-P2-C0 encryption scheme $\mathcal{SE}_1$ having ciphertexts indistinguishable from random) we can weaken the assumption on $W$ to that of a VIL-WMAC. To be more precise, for $V : \{0,1\}^{\kappa_1} \times \{0,1\}^n \times \mathbb{N} \to \{0,1\}^*$ and $W : \{0,1\}^{\kappa_2} \times \{0,1\}^* \to \{0,1\}^\ell$ let $\mathcal{SE}_3$ denote the encryption scheme defined by encrypting $m \in \{0,1\}^*$ under the key $(k_1, k_2) \in \{0,1\}^{\kappa_1} \times \{0,1\}^{\kappa_2}$ as

$$(k_1, k_2, r, m) \mapsto \Big(r, \underbrace{V_{k_1}(r, |m|) \oplus m}_{c}, W_{k_2}(r\|c)\Big), \qquad (\mathcal{SE}_3) \qquad (7)$$

where $r \xleftarrow{\$} \{0,1\}^n$ is auxiliary randomness. The following theorem states that $\mathcal{SE}_3$ is and INT-CTXT- and IND-P2-C2-secure if $V$ is a VOL-WPRF and $W$ is a VIL-WMAC (or a VIL-MAC).

**Theorem 4.** *For any $t, q, \mu, q'$, and $\mu'$*

$$\mathbf{Adv}^{\textbf{ind-p2-c0}}_{\mathcal{SE}_3}(t,q,\mu) \le \mathbf{Adv}^{\textbf{ind-p2-c0}}_{\mathcal{SE}_1}(t,q,\mu)$$

$$\mathbf{Adv}^{\textbf{int-ctxt}}_{\mathcal{SE}_3}(t,q,\mu,q',\mu') \le \min\Big\{\mathbf{Adv}^{\textbf{vol-wprf}}_{V}(t,q,\mu) + \frac{q^2}{2^{n+1}} + q' \cdot \mathbf{Adv}^{\textbf{vil-wmac}}_{W}(t,q,\mu{+}qn{+}\mu'),$$
$$q' \cdot \mathbf{Adv}^{\textbf{vil-mac}}_{W}(t,q,\mu{+}q\delta{+}\mu')\Big\}$$

$$\mathbf{Adv}^{\textbf{ind-p2-c2}}_{\mathcal{SE}_3}(t,q,\mu,q',\mu') \le 2 \cdot \mathbf{Adv}^{\textbf{int-ctxt}}_{\mathcal{SE}_3}(t,q,\mu,q',\mu') + \mathbf{Adv}^{\textbf{ind-p2-c0}}_{\mathcal{SE}_1}(t,q,\mu).$$

An interesting open question for further research is how efficient constructions there are of VIL-WMACs from any WPRF (or WMAC). Next, we briefly discuss a general approach [22] (see also [20, 7]) for constructing a VIL-MAC $W$ (which of course also is a VIL-WMAC) from any PRF. Combining this with $\mathcal{SE}_3$, our PRF $\mathrm{IC}^F$, and VOL-WPRF $\mathrm{ICT}^F$ yields an efficient CCA secure encryption scheme from any WPRF $F$. The idea (for the construction of $W$) is to first hash the message using an $\varepsilon$-almost universal hash function[16] $H : \{0,1\}^{\kappa'} \times \{0,1\}^* \to \{0,1\}^N$ and then to apply $\mathrm{IC}^F : \{0,1\}^\kappa \times \{0,1\}^N \to \{0,1\}^n$ to the result, i.e., $W_{k,k'}(x) := \mathrm{IC}^F_k \circ H_{k'}(x)$.[17] This method is appealing since it is stateless, $H$ exists unconditionally, and the cryptographic function $\mathrm{IC}^F$ is only invoked on short inputs.

*Remark 3.* Damgård and Nielsen [9] also proposed to use the encrypt-then-MAC method for achieving CCA-security of $\mathcal{SE}_1$. However, their approach for constructing the VIL-MAC from any WPRF introduces a too large overhead for the solution to be practical (the number of applications of the WPRF per evaluation is in the order of the message length). Our construction of the VIL-MAC from any $n$-bit block WPRF is more efficient using at most $N$ (or $2N-1$ in case of no pre-processing) applications of the WPRF independently of the message length, where $N \ll n$.[18]

[16] $H$ is $\varepsilon$-almost universal ($\varepsilon$-AU) [21] if for all distinct $m, m' \in \{0,1\}^*$, we have $\Pr[k \leftarrow \mathcal{U}_{\kappa'} : H_k(m) = H_k(m')] \le \varepsilon$.

[17] For any $Q : \{0,1\}^\kappa \times \{0,1\}^N \to \{0,1\}^n$ and $\epsilon$-AU hash function $H : \{0,1\}^{\kappa'} \times \{0,1\}^* \to \{0,1\}^N$ we have that $\mathbf{Adv}^{\textbf{vil-mac}}_{Q \circ H}(t,q,\mu) \le \mathbf{Adv}^{\textbf{prf}}_{Q}(t,q) + q(q-1)\varepsilon/2 + 1/2^n$ (see [7]).

[18] There are $\frac{2}{2^N}$-AU hash functions with key length shorter than $4N$ and maximal input length $2^N$ (see [22]). Hence, as long as $N \in \omega(\log(n))$ the collision probability is sufficiently small for our purposes.

We stress that this additive overhead is of little concern for long messages. Constructing CCA-secure encryption schemes based on WPRFs that is efficient even for very short messages is an open problem.

## 5 Conclusions

We have proposed two constructions (ICT and IC) that are more efficient than prior constructions. Whereas ICT gives an optimal way to extend the output-length of weak PRFs, IC is a construction of a PRF from any weak PRF. These results imply an optimization of Damgård and Nielsen's CPA-secure encryption scheme based on any weak PRF [9], and the first efficient CCA-secure encryption scheme based on any weak PRF. It is an open problem to construct a CCA-secure encryption scheme from any weak PRF, which is efficient even for very short messages. An other open question is whether more efficient constructions of weak MACs based on weak PRFs exist (than the once presented in this paper).

Basing the security on weaker primitives gives not only a better security guarantee. Weaker primitives are also potentially more efficiently implementable than stronger ones. Although several highly efficient candidates for weak PRFs exist, none were targeted at this particular security notion explicitly. It is an interesting question for further research how much block-cipher design can benefit from this weakening of the desired security goal.

## References

1. W. Aiello, S. Rajagopalan, and R. Venkatesan. High-speed pseudorandom number generation with small memory. In *Fast Software Encryption*, volume 1636 of *LNCS*, pages 290–304. Springer, 1999.
2. F. Bao, R. H. Deng, and H. Zhu. Variations of Diffie-Hellman problem. In *ICICS '03*, volume 2836 of *LNCS*, pages 301–312. Springer, 2003.
3. M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A concrete security treatment of symmetric encryption. In *Proc. of the 38th Symposium on Foundations of Computer Science*, pages 394–403. IEEE, 1997.
4. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. In *Advances in Cryptology - CRYPTO '98*, volume 1462 of *LNCS*, pages 26–45. Springer, 1998.
5. M. Bellare, J. Kilian, and P. Rogaway. The security of cipher block chaining. In *Advances in Cryptology - CRYPTO '94*, volume 839 of *LNCS*, pages 341–358. Springer, 1994.
6. M. Bellare and C. Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In *Advances in Cryptology - ASIACRYPT '00*, volume 1976 of *LNCS*, pages 531–545. Springer, 2000.
7. J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway. Umac: Fast and secure message authentication. In *Advances in Cryptology - CRYPTO '99*, volume 1666 of *LNCS*, pages 313–328. Springer, 1999.
8. A. Blum, M. L. Furst, M. J. Kearns, and R. J. Lipton. Cryptographic primitives based on hard learning problems. In *Advances in Cryptology - CRYPTO '93*, volume 773 of *LNCS*, pages 278–291. Springer, 1993.
9. I. Damgård and J. B. Nielsen. Expanding pseudorandom functions; or: from known-plaintext security to chosen-plaintext security. In *Advances in Cryptology - CRYPTO '02*, volume 2442 of *LNCS*, pages 449–464. Springer, 2002.
10. W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.
11. O. Goldreich. *Foundations of Cryptography – Volume II – Basic Applications*. Cambridge University Press, 2004.
12. O. Goldreich, S. Goldwasser, and S. Micali. How to construct random functions. *J. of the ACM*, 33(4):792–807, 1986.
13. J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, 1999.

14. J. Katz and M. Yung. Complete characterization of security notions for probabilistic private-key encryption. In *Proc. of the 32nd Annual Symposium on Theory of Computing*, pages 245–254. ACM, 2000.
15. S. Kent and R. Atkinson. IP encapsulating security payload (ESP). Request for Comments 2406, November 1998.
16. Kazuhiko Minematsu and Yukiyasu Tsunoo. Expanding weak PRF with small key size. In *Information Security and Cryptology — ICISC '05*, volume 3935 of *LNCS*, pages 284–298. Springer, 2005.
17. M. Naor and O. Reingold. From unpredictability to indistinguishability: A simple construction of pseudo-random functions from MACs. In *Advances in Cryptology - CRYPTO '98*, volume 1462 of *LNCS*, pages 267–282. Springer, 1998.
18. M. Naor and O. Reingold. Synthesizers and their application to the parallel construction of pseudo-random functions. *J. Comput. Syst. Sci*, 58(2):336–375, 1999.
19. M. Naor and O. Reingold. Number-theoretic constructions of efficient pseudo-random functions. *J. of the ACM*, 51(2):231–262, 2004.
20. V. Shoup. On fast and provably secure message authentication based on universal hashing. In *Advances in Cryptology - CRYPTO '96*, volume 1109 of *LNCS*, pages 313–328. Springer, 1996.
21. D. R. Stinson. Universal hashing and authentication codes. In *Advances in Cryptology - CRYPTO '91*, volume 576 of *LNCS*, pages 74–85. Springer, 1992.
22. M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. *J. of Computer and System Sciences*, 22:265–279, 1981.

## A Proof of Theorem 1

*Proof (of Theorem 1).* Let $\Pi_0$ denote the following game for an adversary $A$ with resources $(t, q)$:

$$(k, r, r') \xleftarrow{\$} \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n,\ b \leftarrow A^{\mathrm{IC}^F_{k,r,r'}}.$$

Recall the algorithm describing $\mathrm{IC}^F$ on page 6. For $j = \{1, \ldots, N\}$, let $\Pi_{2j-1}$ be the same game as $\Pi_{2j-2}$, except that $F_{k_j}$ is replaced by a random function, and let $\Pi_{2j}$ be the same game as $\Pi_{2j-1}$, except that $k_j$ is replaced by a random string and for each query $x$ to $\mathrm{IC}^F$ the intermediate value $\tau_j$ is replaced by a random string unless $x[1, j]$ is not a prefix of an earlier query. Finally, note that $\Pi_{2N}$ is equivalent to

$$R \leftarrow \mathcal{R}_{N,n},\ b \leftarrow A^R.$$

Let $S_j$ denote the event that $b = 1$ in $\Pi_j$ (for $j \in \{0, \ldots, 2N\}$). Then

$$\begin{aligned}
\mathbf{Adv}^{\mathbf{prf}}_{\mathrm{IC}^F,A} := \big|\Pr[S_0]-\Pr[S_{2N}]\big| &\le \sum_{j=1}^{N}\Big(\big|\Pr[S_{2j-2}]-\Pr[S_{2j-1}]\big| + \big|\Pr[S_{2j-1}]-\Pr[S_{2j}]\big|\Big)\\
&\le \sum_{j=1}^{N}\mathbf{Adv}^{\mathbf{wprf}}_F\big(t, \min\{q+1, 2^{j-1}+1\}\big) + \min\left\{\frac{(q+1)q}{2^{n+1}}, \frac{(2^{j-1}+1)2^{j-1}}{2^{n+1}}\right\}\\
&\le N\cdot\left(\mathbf{Adv}^{\mathbf{wprf}}_F(t, q+1) + \frac{q(q+1)}{2^{n+1}}\right),
\end{aligned}$$

which follows from the triangle inequality, the easily verified fact that $A$ can be transformed to a **wprf**-distinguisher (restricted to time-complexity $t$ and most $\min(q+1, 2^{j-1}+1)$ oracle invocations) which has advantage at least $\Pr[S_{2j-2}] - \Pr[S_{2j-1}]$, and the fact that $\Pi_{2j-1}$ and $\Pi_{2j}$ (for all $j \in \{1, \ldots, N\}$) are equivalent games as long as $r$ and the assignments of the variable $\tau_{j-1}$ in the algorithm are all distinct. The probability of this event is upper bounded by $\min\big\{(q+1)q/2^{n+1}, (2^{j-1}+1)2^{j-1}/2^{n+1}\big\}$, as these values are at most $\min\{q+1, 2^{j-1}+1\}$ and distributed uniformly at random. □

## B Proof of Theorem 2 (and two PRGs from any WPRF)

For any function $f : \{0,1\}^n \to \{0,1\}^n$ and bitstring $\mathbf{x} = x_1 \| \cdots \| x_s \in \{0,1\}^{sn}$, where $x_1, \ldots, x_s$ are $n$-bit blocks, let $f(\mathbf{x}) := f(x_1) \| \cdots \| f(x_q)$. If $\mathcal{D}_1$ and $\mathcal{D}_2$ are two probability distributions over $S$, then let the distinguishing advantage of a distinguisher $A$ be defined as

$$\mathbf{Adv}_A^{\mathcal{D}_1,\mathcal{D}_2} := \left| \Pr[s \leftarrow \mathcal{D}_1, b \leftarrow A(s) : b = 1] - \Pr[s \leftarrow \mathcal{D}_2, b \leftarrow A(s) : b = 1] \right|,$$

and the maximal distinguishing advantage as

$$\mathbf{Adv}^{\mathcal{D}_1,\mathcal{D}_2}(t) := \max_A \{\mathbf{Adv}_A^{\mathcal{D}_1,\mathcal{D}_2}\},$$

where the maximum is taken over all $D$ with time-complexity $t$.

Before we present the proof of Theorem 2, let us consider the following two constructions of PRGs from any WPRF $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ and any nonzero $s$, $d \in \mathbb{N}$:

$$\begin{aligned} G_s^F &: \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^{sn} \to \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^{2sn} \\ &(k, r, \mathbf{x}) \mapsto (F_k(r), r, \mathbf{x} \| F_k(\mathbf{x})) \end{aligned} \tag{8}$$

$$\begin{aligned} G_{s,d}^F &: \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^{sn} \to \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^{2^d sn} \\ &(k, r, \mathbf{x}) \mapsto G_{s2^{(d-2)}}^F \circ G_{s2^{d-1}}^F \circ \cdots \circ G_{s2^0}^F(k, r, \mathbf{x}). \end{aligned} \tag{9}$$

The following two lemmata state that the above constructions are PRGs if $F$ is a WPRF.

**Lemma 1.** *For any $t$ and $s > 0$*

$$\mathbf{Adv}_{G_s^F}^{\mathbf{prg}}(t) \leq \mathbf{Adv}_F^{\mathbf{wprf}}(t, s+1) + \frac{s(s+1)}{2^{n+1}}.$$

*Proof.* Consider the following three distributions:

$$\mathcal{D}_1 := F_k(r) \,\|\, r \,\|\, \mathbf{x} \,\|\, F_k(\mathbf{x}), \quad \mathcal{D}_2 := R(r) \,\|\, r \,\|\, \mathbf{x} \,\|\, R(\mathbf{x}), \quad \text{and} \quad \mathcal{D}_3 := \mathcal{U}_{2(s+1)n},$$

where $r \| \mathbf{x} \leftarrow \mathcal{U}_{(s+1)n}$ and $R \leftarrow \mathcal{R}_{n,n}$. Then

$$\begin{aligned} \mathbf{Adv}_{G_s^F}^{\mathbf{prg}}(t) = \mathbf{Adv}^{\mathcal{D}_1,\mathcal{D}_3}(t) &\leq \mathbf{Adv}^{\mathcal{D}_1,\mathcal{D}_2}(t) + \mathbf{Adv}^{\mathcal{D}_2,\mathcal{D}_3}(t) \\ &\leq \mathbf{Adv}_F^{\mathbf{wprf}}(t, s+1) + \frac{s(s+1)}{2^{n+1}}, \end{aligned}$$

which follows directly from the triangle inequality, the fact that $\mathcal{D}_2$ and $\mathcal{D}_3$ are the same distributions as long as the values $r, x_1, \ldots, x_s$ are all distinct (an event upper bounded by $s(s+1)/2^{n+1}$), and the trivial fact that any distinguisher for $\mathcal{D}_1$, $\mathcal{D}_2$ can be transformed into a **wprf**-adversary (for $F$) which makes $s+1$ oracle invocations, and has the same advantage and time-complexity. □

**Lemma 2.** *For any $t$ and $s, d > 0$*

$$\mathbf{Adv}_{G_{s,d}^F}^{\mathbf{prg}}(t) \leq d \cdot \mathbf{Adv}_F^{\mathbf{wprf}}(t, s2^{d-1} + 1) + \frac{s^2 \cdot (4^d - 1)}{2^{n+1}}.$$

*Proof.* The proof follows from a simple hybrid argument and Lemma 1.

$$\begin{aligned}\mathbf{Adv}^{\mathbf{prg}}_{G^F_{s,d}}(t) &\le \sum_{i=0}^{d-1} \mathbf{Adv}^{\mathbf{prg}}_{G^F_{s2^i}}(t) \le \sum_{i=0}^{d-1}\left(\mathbf{Adv}^{\mathbf{wprf}}_{F}(t, s2^i+1) + \frac{s2^i\,(s2^i+1)}{2^{n+1}}\right)\\ &\le d\cdot \mathbf{Adv}^{\mathbf{wprf}}_{F}(t, s2^{d-1}+1) + \frac{1}{2^{n+1}}\underbrace{\left(\frac{s^2\,(4^d-1)}{3} + s\cdot(2^d-1)\right)}_{\le s^2\cdot(4^d-1)}.\end{aligned}$$

□

*Proof (of Theorem 2).* Note that the ICT-construction can similarly be defined as follows. For any $l \in \mathbb{N}$, let $d = \lfloor \log_2(\lceil l/n \rceil)\rfloor + 1$. Then

$$\begin{aligned}\mathrm{ICT}^F : \{0,1\}^{2n} \times \{0,1\}^n \times \mathbb{N} &\to \{0,1\}^*\\ (k\|r, x, l) &\mapsto \tilde{G}^F_{1,d}(k,r,x)[1,l],\end{aligned}$$

where $\tilde{G}^F_{s,d}(k,r,\mathbf{x})$ is defined by $G^F_{s,d}(k,r,\mathbf{x}) = (k', r, \mathbf{x}\|\tilde{G}^F_{s,d}(k,r,\mathbf{x}))$, i.e., the first two output-components of $G^F_{s,d}(k,r,\mathbf{x})$ and $\mathbf{x}$ are not an output.

Let $r, k, x_1, \ldots, x_q \leftarrow \mathcal{U}_n$, $l_i \in \mathbb{N}$ the length of the $i^{\text{th}}$ output, $l_{\max}$ the maximal allowed output length of $\mathrm{ICT}^F$, and $d_{\max} := \lfloor \log_2(\lceil l_{\max}/n \rceil)\rfloor + 1$. For $R \leftarrow \mathcal{R}_{n,*}$, consider the following distributions where $A \sqsubseteq B$ indicates that distribution $A$ can be sampled with help of $B$, by first sampling from $B$ and then removing and reranging bits of the sample.

$$\begin{aligned}\mathcal{D}_1 &:= x_1\|\cdots\|x_q\|\, R(x_1,l_1) \qquad\qquad \|\cdots\|\; R(x_q,l_q)\\ \mathcal{D}_2 &:= x_1\|\cdots\|x_q\|\; \mathrm{ICT}^F(k\|r,x_1,l_1) \quad\;\; \|\cdots\|\; \mathrm{ICT}^F(k\|r,x_q,l_q)\\ &= x_1\|\cdots\|x_q\|\; \tilde{G}^F_{1,\,d_{\max}}(k,r,x_1)[1,l_1]\,\|\cdots\|\; \tilde{G}^F_{1,\,d_{\max}}(k,r,x_q)[1,l_q]\\ &\sqsubseteq x_1\|\cdots\|x_q\|\; \tilde{G}^F_{q,d_{\max}}(k,r,x_1\|\cdots\|x_q) \sqsubseteq G^F_{q,d_{\max}}(k,r,\mathbf{x}) =: \mathcal{D}'_2\\ \mathcal{D}_3 &:= \mathcal{U}_{qn+l_1+\cdots+l_q} \qquad\qquad\qquad\qquad\quad \sqsubseteq \mathcal{U}_{(2+q2^{d_{\max}})\cdot n} \quad =: \mathcal{D}'_3\,.\end{aligned}$$

By the triangle inequality and Lemma 2 it follows that when[19] $t' = t + \mathcal{O}(\frac{q\cdot l_{\max}}{n}\cdot t_F)$

$$\begin{aligned}\mathbf{Adv}^{\textbf{vol-wprf}}_{\mathrm{ICT}^F}(t,q,\mu) &\le \mathbf{Adv}^{\mathcal{D}_1,\mathcal{D}_3}(t') + \mathbf{Adv}^{\mathcal{D}'_2,\mathcal{D}'_3}(t') \le \frac{q(q-1)}{2^{n+1}} + \mathbf{Adv}^{\mathbf{prg}}_{G^F_{q,d_{\max}}}(t')\\ &\le \frac{q(q-1)}{2^{n+1}} + d\cdot\mathbf{Adv}^{\mathbf{wprf}}_{F}(t', s2^{d_{\max}-1}+1) + \frac{q^2\cdot(4^{d_{\max}}-1)}{2^{n+1}}.\end{aligned}$$

□

*Remark 4 (Reduction of key material).* All the (initial) keys of our constructions (in this paper) can be generated from a WPRF $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, two publicly random domain points (i.e., two $n$-bit strings $r$ and $r'$), and a secret key $k$ of $F$. To generate $t$ ($n$-bit) keys $k_1, \ldots, k_t$ one simply computes $k_1\|\ldots\|k_t := \mathrm{ICT}^F_{k\|r}(r', tn)$. This follows from the fact that

$$(r, r', k) \mapsto r\|r'\|\,\mathrm{ICT}^F_{k\|r}(r', tn) = G^F_{1,\lceil \log_2(t)\rceil}(k,r,r')[n{+}1,(t{+}3)n] \tag{10}$$

is a PRG for any fixed $t > 1$, according to Lemma 2. This key generation method is more efficient and uses a shorter key than the method presented in [9].

*Remark 5.* To construct a length doubling PRG from a WPRF $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, we simply set $t = 4$ in (10). This results in a PRG $\{0,1\}^{3n} \to \{0,1\}^{6n}$ which invokes $F$ 6 times (i.e., in the computation of $\mathrm{ICT}^F_{k\|r}(r', 4n)$).

[19] The worst-case running time for sampling $\mathcal{D}_1$, $\mathcal{D}'_2$, or $\mathcal{D}'_3$ is in $\mathcal{O}(\frac{q\cdot l_{\max}}{n}\cdot t_F)$.

## C Proof of Proposition 1, Theorem 3, and Theorem 4

*Proof (of Proposition 1).* Recall that $\mathcal{SE}_1 = (E, D)$ is defined as $E_k(m) := (r, V_k(r, |m|) \oplus m)$, where $V$ is a VOL function family. Let $\Pi_0$ denote the IND-P2-C0 game for any adversary $A$ with resources $(t, q, \mu)$, i.e.,

$$k \overset{\$}{\leftarrow} \{0,1\}^{\kappa};\ (x_0, x_1) \leftarrow A^{E_k};\ b \overset{\$}{\leftarrow} \{0,1\};\ y \leftarrow E_k(x_b);\ \hat{b} \leftarrow A^{E_k}(y).$$

Furthermore, let $\Pi_1$ be the same game as $\Pi_0$, except that $V_k$ is replaced by $\mathcal{R}_{\mathrm{n},*}$. Let $\Pi_2$ be the same game as $\Pi_1$, except that the input $y$ to the adversary is replaced by a truly random string $y'$ of the same length. For $i \in \{0, 1, 2\}$ let $S_i$ denote the event that $\hat{b} = b$ in game $\Pi_i$. Then

$$\begin{aligned}\mathbf{Adv}^{\textbf{ind-p2-c0}}_{\mathcal{SE}_1,A} &:= 2 \cdot \Pr[S_0] - 1 = 2\left(\Pr[S_2] + \sum_{i=0}^{1} \Pr[S_i] - \Pr[S_{i+1}]\right) - 1\\ &\leq 2 \cdot \left(\frac{1}{2} + \mathbf{Adv}^{\textbf{vol-wprf}}_{V}(t, q, \mu) + \frac{q-1}{2^n}\right) - 1,\end{aligned}$$

where the inequality follows from the easily verified fact that $A$ implies a distinguisher $A'$ for $V$ with the same resources and advantage at least $\Pr[S_0] - \Pr[S_1]$ ($A'$ simply runs $A$ answering its oracle queries with help of its own oracle in place of $V$ and returns whatever $A$ does), the fact that $\Pi_1$ and $\Pi_2$ are equivalent games as long as the input to $\mathcal{R}_{\mathrm{n},*}$ in the computation of $y$ is different from the other inputs to $\mathcal{R}_{\mathrm{n},*}$ (an event upper bounded by $(q-1)/2^n$), and that $\Pr[S_2] = 1/2$ since $b$ is independent of $y$. □

*Proof (of Theorem 3).* Recall that $\mathcal{SE}_2 = (E, D)$ is defined as

$$E_{k_1,k_2}(m) := \big(r, V_{k_1}(r, |m|) \oplus m, W_{k_2}(r)\big),$$

where $V$ is a VOL-WPRF and $W$ is a WMAC. We prove the second inequality (the proof of the first inequality is straight forward and therefore omitted).

Let $\Pi_0$ denote the IND-P2-C1 game for any adversary $A$ with resources $(t, q, \mu, q', \mu')$, i.e.,

$$\begin{aligned}&(k_1, k_2) \overset{\$}{\leftarrow} \{0,1\}^{\kappa_1} \times \{0,1\}^{\kappa_2},\\ &(x_0, x_1) \leftarrow A^{E_{k_1,k_2}, D_{k_1,k_2}},\\ &b \overset{\$}{\leftarrow} \{0,1\}, y \leftarrow E_{k_1,k_2}(x_b),\\ &\hat{b} \leftarrow A^{E_{k_1,k_2}}(y).\end{aligned}$$

Furthermore, let $\Pi_1$ be the same game as $\Pi_0$, except that all decryption queries, for which the auxiliary random part $r$ is distinct from the auxiliary random parts $r_1, r_2, \ldots$ of the ciphertexts received from the encryption oracle, are rejected. Furthermore, let $S_i$, for $i \in \{0, 1\}$, denote the event that $\hat{b} = b$ in $\Pi_i$. Then

$$\begin{aligned}\mathbf{Adv}^{\textbf{ind-p2-c1}}_{\mathcal{SE}_2,A} &:= 2 \cdot \Pr[S_0] - 1 = 2 \cdot \Big(\Pr[S_0] - \Pr[S_1]\Big) + 2 \cdot \Pr[S_1] - 1\\ &\leq 2 \cdot \Pr[\mathcal{E}] + \mathbf{Adv}^{\textbf{ind-p2-c0}}_{\mathcal{SE}_2}(t, q, \mu),\end{aligned}$$

where $\mathcal{E}$ denotes the event that $A$ queries a valid ciphertext to its decryption oracle for which the $r$-value is distinct from the once returned from the encryption oracle. The inequality follows from the fact that $\mathit{\Pi}_0$ and $\mathit{\Pi}_1$ are equivalent games unless $\mathcal{E}$ occurs and that the decryption queries do not help the adversary in $\mathit{\Pi}_1$ since the adversary can simulate the decryption oracle itself. It remains to show that

$$\Pr[\mathcal{E}] \leq q' \cdot \mathbf{Adv}_W^{\mathbf{wmac}}(t, q).$$

This follows from the fact that $A$ can be transformed to a forger $A'$ for $W$ with advantage at least $\Pr[\mathcal{E}]/q'$ using the resources $(t, q)$ as follows. $A'$ picks a random $i \in \mathbb{Z}_{q'}$ and runs $A$ answering its encryption oracle queries with help of its own oracle and rejecting the first $i$ queries to the decryption oracle. If $A$ presents its challenge input $(m_0, m_1)$, $A'$ flips a coin, encrypts $m_b$ with help of its own oracle, and returns the resulting ciphertext to $A$. $A'$ returns $A$'s $(i+1)$-th query to the decryption oracle as its forgery. □

*Proof (of Theorem 4).* Recall that $\mathcal{SE}_3 = (E, D)$ is defined as

$$E_{k_1,k_2}(m) := \big(r, \underbrace{V_{k_1}(r, |m|) \oplus m}_{c}, W_{k_2}(r\|c)\big).$$

We prove the second and third inequality (we omit the proof of the first as it is straight forward).

Let $\mathit{\Pi}_0$ denote the INT-CTXT game for any adversary $A$ with resources $(t, q, \mu, q', \mu')$, i.e.,

$$(k_1, k_2) \overset{\$}{\leftarrow} \{0,1\}^{\kappa_1} \times \{0,1\}^{\kappa_2},\ A^{E_{k_1,k_2}, D^*_{k_1,k_2}}.$$

Let $\mathit{\Pi}_1$ denote the same game as $\mathit{\Pi}_0$ except that $V$ has been replaced by $R_{n,*}$. Furthermore, let $\mathit{\Pi}_2$ be the same game as $\mathit{\Pi}_1$ except that the output of $R_{n,*}$ is replaced by a truly random string (no matter of the input). Let $\mathcal{E}_i$ denote the event that $D^*$ outputs 1 in $\mathit{\Pi}_i$ for $i \in \{0, 1, 2\}$. Then

$$\begin{aligned}\mathbf{Adv}_{\mathcal{SE}_3,A}^{\textbf{int-ctxt}} = \Pr[\mathcal{E}_0] &\leq \Big|\Pr[\mathcal{E}_0] - \Pr[\mathcal{E}_1]\Big| + \Big|\Pr[\mathcal{E}_1] - \Pr[\mathcal{E}_2]\Big| + \Pr[\mathcal{E}_2] \\ &\leq \mathbf{Adv}_V^{\textbf{vol-wprf}}(t, q, \mu) + \frac{(q-1)q}{2^{n+1}} + q' \cdot \mathbf{Adv}_W^{\textbf{vil-wmac}}(t, q, \mu + qn + \mu').\end{aligned}$$

The inequality follows from the following three facts. First, $A$ implies a **vol-wprf**-distinguisher $A'$ for $V$ with advantage $|\Pr[\mathcal{E}_0] - \Pr[\mathcal{E}_1]|$ and resources $(t, q, \mu)$. $A'$ simply runs $A$ answering its oracle queries with help of its own oracle in place of $V$ and iff $A$ is successful $A'$ outputs 1. Second, $\mathit{\Pi}_1$ and $\mathit{\Pi}_2$ are equivalent games unless the auxiliary random $r$-values are not all distinct, an event upper bounded by $q(q-1)/2^{n+1}$. Finally, from $A$ we can construct a **vil-wmac**-forger $A''$ for $W$ with advantage $\Pr[\mathcal{E}_2]/q'$ and resources $(t, q, \mu + qn + \mu')$. $A''$ picks a random element $i \in \mathbb{Z}_{q'}$ and simply runs $A$ answering its queries to $E$ with help of its own oracle and rejecting its first $i$ queries to $D^*$. When $A$ makes its $(i+1)$-th query to $D^*$, $A''$ returns it as its forgery. Similarly, one can show that $A$ implies a **vil-mac**-forger for $W$ with advantage $\Pr[\mathcal{E}_0]/q'$ and resources $(t, q, \mu + qn + \mu')$. Hence

$$\mathbf{Adv}_{\mathcal{SE}_3,A}^{\textbf{int-ctxt}} = \Pr[\mathcal{E}_0] \leq q' \cdot \mathbf{Adv}_W^{\textbf{vil-mac}}(t, q, \mu + qn + \mu').$$

Let $\mathit{\Pi}'_0$ denote the IND-P2-C2 game for any adversary $A$ with resources $(t, q, \mu, q', \mu')$, i.e.,

$$\begin{aligned}
&(k_1, k_2) \overset{\$}{\leftarrow} \{0,1\}^{\kappa_1} \times \{0,1\}^{\kappa_2},\\
&(x_0, x_1) \leftarrow A^{E_{k_1,k_2}, D_{k_1,k_2}},\\
&b \overset{\$}{\leftarrow} \{0,1\}, y \leftarrow E_{k_1,k_2}(x_b),\\
&\hat{b} \leftarrow A^{E_{k_1,k_2}, D_{k_1,k_2}}(y).
\end{aligned}$$

Let $\mathit{\Pi}'_1$ be the same game as $\mathit{\Pi}'_0$, except that all decryption queries are rejected. Moreover, let $S_i$ for $i \in \{0,1\}$ denote the event that $\hat{b} = b$ in $\mathit{\Pi}'_i$. Then

$$\begin{aligned}
\mathbf{Adv}^{\textbf{ind-p2-c2}}_{\mathcal{SE}_3, A} &:= 2 \cdot \Pr[S_0] - 1 = 2 \cdot \Big(\Pr[S_0] - \Pr[S_1]\Big) + 2 \cdot \Pr[S_1] - 1\\
&\leq 2 \cdot \Pr[\mathcal{E}] + \mathbf{Adv}^{\textbf{ind-p2-c0}}_{\mathcal{SE}_3}(t, q, \mu),
\end{aligned}$$

where $\mathcal{E}$ denotes the event that a query to the decryption oracle in $\mathit{\Pi}'_1$ (or $\mathit{\Pi}'_0$) is correctly formed (and hence not rejected). The inequality follows from the the fact that $\mathit{\Pi}'_0$ and $\mathit{\Pi}'_1$ are equivalent games unless $\mathcal{E}$ occurs, and since $\mathit{\Pi}'_1$ is the IND-P2-C0 game. It remains to show that

$$\Pr[\mathcal{E}] \leq \mathbf{Adv}^{\textbf{int-ctxt}}_{\mathcal{SE}_3}(t, q, \mu, q', \mu').$$

This is the case as $A$ can trivially be transformed into a **int-ctxt**-adversary $A'''$ (for $\mathcal{SE}_3$) using the same resources and having advantage $\Pr[\mathcal{E}]$. $A'''$ simply runs $A$ and forwards the encryption (decryption) queries to its own encryption (decryption*) oracle. If $A$ presents its challenge input $(m_0, m_1)$, $A'''$ flips a coin, queries its encryption oracle with $m_b$, and returns the result to $A$. □