Countermeasures Against High-Order Fault-Injection Attacks on CRT-RSA

Pablo Rauzy, Sylvain Guilley

Countermeasures Against High-Order Fault-Injection Attacks on CRT-RSA

Pablo Rauzy and Sylvain Guilley
Institut Mines-Télécom ; Télécom ParisTech ; CNRS LTCI
{*firstname.lastname*}@telecom-paristech.fr

Abstract

In this paper we study the existing CRT-RSA countermeasures against fault-injection attacks. In an attempt to classify them we get to achieve deep understanding of how they work. We show that the many countermeasures that we study (and their variations) actually share a number of common features, but optimize them in different ways. We also show that there is no conceptual distinction between test-based and infective countermeasures and how either one can be transformed into the other. Furthermore, we show that faults on the code (skipping instructions) can be captured by considering only faults on the data. These intermediate results allow us to improve the state of the art in several ways: (a) we fix an existing and that was known to be broken countermeasure (namely the one from Shamir); (b) we drastically optimize an existing countermeasure (namely the one from Vigilant) which we reduce to 3 tests instead of 9 in its original version, and prove that it resists not only one fault but also an arbitrary number of randomizing faults; (c) we also show how to upgrade countermeasures to resist any given number of faults: given a correct first-order countermeasure, we present a way to design a provable high-order countermeasure (for a well-defined and reasonable fault model). Finally, we pave the way for a generic approach against fault attacks for any modular arithmetic computations, and thus for the automatic insertion of countermeasures.

1 Introduction

Private information protection is a highly demanded feature, especially in the current context of global defiance against most infrastructures, assumed to be controlled by governmental agencies. Properly used cryptography is known to be a key building block for secure information exchange. However, in addition to the threat of cyber-attacks, implementation-level hacks must also be considered seriously. This article deals specifically with the protection of a *decryption* or *signature* crypto-system (called RSA [**?**]) in the presence of hardware attacks (*e.g.*, we assume the attacker can alter the RSA computation while it is being executed).

It is known since 1997 (with the BellCoRe attack by Boneh *et al.* [**?**]) that injecting faults during the computation of CRT-RSA (CRT for "Chinese Remainder Theorem") could yield to malformed signatures that expose the prime factors (p and q) of the public modulus ($N = p \cdot q$). Notwithstanding, computing without the fourfold acceleration conveyed by the CRT optimization is definitely not an option in practical applications. Therefore, many countermeasures have appeared. Most of the existing countermeasures were designed with an attack-model consisting in a single fault injection. The remaining few attempts to protect against second-order fault attacks (*i.e.*, attacks with two faults).

Looking at the history of the development of countermeasures against the BellCoRe attack, we see that many countermeasures are actually broken in the first place. Some of them were fixed by their authors and/or other people, such as the countermeasure proposed by Vigilant [**?**], which was fixed by Coron *et al.* [**?**] and then simplified by Rauzy & Guilley [**?**]; some simply abandoned, such as the one by Shamir [**?**]. Second-order countermeasures are no exception to that rule, as demonstrated with the countermeasure proposed by Ciet & Joye [**?**], which was fixed later by Dottax *et al.* [**?**]. Such mistakes can be explained by two main points:

- the almost nonexistent use of formal methods in the field of implementation security, which can itself be explained by the difficulty to properly model the physical properties of an implementation which are necessary to study side-channel leakages and fault-injection effects;
- the fact that most countermeasures were developed by trial-and-error engineering, accumulating layers of intermediate computations and verifications to patch weaknesses until a fixed point was reached, even if the inner workings of the countermeasure were not fully understood.

Given their development process, it is likely the case that existing second-order countermeasures would not resist third-order attacks, and strengthening them against such attacks using the same methods will not make them resist fourth-order, *etc.*

The purpose of this paper is to remedy to these problems. First-order countermeasures have started to be formally studied by Christofi *et al.* [**?**], who have been followed by Rauzy & Guilley [**?**, **?**], and Barthe *et al.* [**?**]. To our best knowledge, no such work has been attempted on high-order countermeasures. Thus, we should understand the working factors of a countermeasure, and use that knowledge to informedly design a generic high-order countermeasure, either one resisting any number of faults, or one which could be customized to protect against n faults, for any given $n \geqslant 1$.

Notice that we consider RSA used in a mode where the BellCoRe attack is applicable; this means that we assume that the attacker can choose (but not necessarily knows) the message that is exponentiated, which is the case in *decryption* mode or in (outdated) *deterministic signature* mode (*e.g.*, PKCS #1 v1.5). In some other modes, formal proofs of security have been conducted [**?**, **?**].

Contributions In this paper we propose a classification of the existing CRT-RSA countermeasures against the BellCoRe fault-injection attacks. Doing so, we raise questions whose answers lead to a deeper understanding of how the countermeasures work. We show that the many countermeasures that we study (and their variations) are actually applying a common protection strategy but optimize it in different ways (Sec. 4). We also show that there is no conceptual distinction between test-based and infective countermeasures and how either one can be transformed into the other (Prop. 2). Furthermore, we show that faults on the code (skipping instructions) can be captured by considering only faults on the data (Lem. 1). These intermediate results allow us to improve the state of the art in several ways:

- we fix an existing and that is known to be broken countermeasure (Alg. 10);
- we drastically optimize an existing countermeasure, while at the same time we transform it to be infective instead of test-based (Alg. 11);
- we also show how to upgrade countermeasures to resist any given number of faults: given a correct first-order countermeasure, we present a way to design a provable high-order countermeasure for a well defined and reasonable fault model (Sec. 4.2).

Finally, we pave the way for a generic approach against fault attacks for any modular arithmetic computations, and thus for the automatic insertion of countermeasures.

Organization of the paper We recall the CRT-RSA cryptosystem and the BellCoRe attack in Sec. 2. Then, to better understand the existing countermeasures, we attempt to classify them in Sec. 3, which also presents the state of the art. We then try to capture what make the essence of a countermeasure in Sec. 4, and use that knowledge to determine how to build a high-order countermeasure. We last use our findings to build better countermeasures by fixing and simplifying existing ones in Sec. 5. Conclusions and perspectives are drawn in Sec. 6. The appendices contain the detail of some secondary results.

2 CRT-RSA and the BellCoRe Attack

This section summarizes known results about fault attacks on CRT-RSA (see also [**?**], [**?**, Chap. 3] and [**?**, Chap. 7 & 8]). Its purpose is to settle the notions and the associated notations that will be used in the later sections, to present our novel contributions.

2.1 RSA

RSA is both an *encryption* and a *signature* scheme. It relies on the fact that for any message $0 \leq M < N$, $(M^d)^e \equiv M \mod N$, where $d \equiv e^{-1} \mod \varphi(N)$, by Euler's theorem[1]. In this equation, φ is Euler's totient function, equal to $\varphi(N) = (p-1) \cdot (q-1)$ when $N = p \cdot q$ is a composite number, product of two primes p and q. For example, if Alice generates the signature $S = M^d \mod N$, then Bob can verify it by computing $S^e \mod N$, which must be equal to M unless Alice is only pretending to know d. Therefore (N, d) is called the private key, and (N, e) the public key. In this paper, we are not concerned about the key generation step of RSA, and simply assume that d is an unknown number in $[\![1, \varphi(N) = (p-1) \cdot (q-1)[\![$. Actually, d can also be chosen to be equal to the smallest value $e^{-1} \mod \lambda(N)$, where $\lambda(N) = \frac{(p-1)\cdot(q-1)}{\gcd(p-1,q-1)}$ is the Carmichael function (see PKCS #1 v2.1, §3.1).

2.2 CRT-RSA

The computation of $M^d \mod N$ can be speeded-up by a factor of four using the Chinese Remainder Theorem (CRT). Indeed, numbers modulo p and q are twice as short as those modulo N. For example, for $2,048$ bits RSA, p and q are $1,024$ bits long. CRT-RSA consists in computing $S_p = M^d \mod p$ and $S_q = M^d \mod q$, which can be recombined into S with a limited overhead. Due to the little Fermat theorem (the special case of the Euler theorem when the modulus is a prime), $S_p = (M \mod p)^{d \mod (p-1)} \mod p$. This means that in the computation of S_p, the processed data have $1,024$ bits, and the exponent itself has $1,024$ bits (instead of $2,048$ bits). Thus the multiplication is four times faster and the exponentiation eight times faster. However, as there are two such exponentiations (modulo p and q), the overall CRT-RSA is roughly speaking four times faster than RSA computed modulo N.

This acceleration justifies that CRT-RSA is always used if the factorization of N as $p \cdot q$ is known. In CRT-RSA, the private key has a richer structure than simply (N, d): it is actually the 5-tuple (p, q, d_p, d_q, i_q), where:

- $d_p \doteq d \mod (p-1)$,

[1] We use the usual convention in all mathematical equations, namely that the "mod" operator has the lowest binding precedence, *i.e.*, $a \times b \mod c \times d$ represents the element $a \times b$ in $\mathbb{Z}_{c \times d}$.

- $d_q \doteq d \mod (q-1)$, and
- $i_q \doteq q^{-1} \mod p$.

The CRT-RSA algorithm is presented in Alg. 1. It is straightforward to check that the signature computed at line 3 belongs to $[\![0, p \cdot q - 1]\!]$. Consequently, no reduction modulo N is necessary before returning S.

Algorithm 1: Unprotected CRT-RSA

Input : Message M, key (p, q, d_p, d_q, i_q)
Output: Signature $M^d \mod N$

1 $S_p = M^{d_p} \mod p$ `// Intermediate signature in` $\mathbb{Z}_p$
2 $S_q = M^{d_q} \mod q$ `// Intermediate signature in` $\mathbb{Z}_q$
3 $S = S_q + q \cdot (i_q \cdot (S_p - S_q) \mod p)$ `// Recombination in` $\mathbb{Z}_N$ `(Garner's method [?])`
4 **return** S

2.3 The BellCoRe Attack

In 1997, a dreadful remark has been made by Boneh, DeMillo and Lipton [**?**], three staff of Bell Communication Research: Alg. 1 could reveal the secret primes p and q if the line 1 or 2 of the computation is faulted, even in a very random way. The attack can be expressed as the following proposition.

Proposition 1 (BellCoRe attack)**.** *If the intermediate variable S_p (resp. S_q) is returned faulted as $\widehat{S_p}$ (resp. $\widehat{S_q}$)*[2]*, then the attacker gets an erroneous signature $\widehat{S}$, and is able to recover q (resp. p) as* $\gcd(N, S - \widehat{S})$.

Proof. For any integer x, $\gcd(N, x)$ can only take 4 values:
- 1, if N and x are coprime,
- p, if x is a multiple of p,
- q, if x is a multiple of q,
- N, if x is a multiple of both p and q, *i.e.*, of N.

In Alg. 1, if S_p is faulted (*i.e.*, replaced by $\widehat{S_p} \neq S_p$), then $S - \widehat{S} = q \cdot ((i_q \cdot (S_p - S_q) \mod p) - (i_q \cdot (\widehat{S_p} - S_q) \mod p))$, and thus $\gcd(N, S - \widehat{S}) = q$. If S_q is faulted (*i.e.*, replaced by $\widehat{S_q} \neq S_q$), then $S - \widehat{S} \equiv (S_q - \widehat{S_q}) - (q \mod p) \cdot i_q \cdot (S_q - \widehat{S_q}) \equiv 0 \mod p$ because $(q \mod p) \cdot i_q \equiv 1 \mod p$, and thus $S - \widehat{S}$ is a multiple of p. Additionally, $S - \widehat{S}$ is not a multiple of q. So, $\gcd(N, S - \widehat{S}) = p$. □

Before continuing to the next section, we will formalize our attack model by defining what is a fault injection and what is the order of an attack.

Definition 1 (Fault injection)**.** During the execution of an algorithm, the attacker can:

[2] In other papers, the faulted variables (such as X) are written either as X^* or $\tilde{X}$; in this paper, we use a hat which can stretch to cover the adequate portion of the expression, as it allows to make an unambiguous difference between $\widehat{X^e}$ and $\widehat{X}^e$.

- modify any intermediate value by setting it to either a *random value* (*randomizing fault*) or *zero* (*zeroing fault*); such a fault can be either *permanent* (*e.g.*, in memory) or *transient* (*e.g.*, in a register or a bus);
- skip any number of consecutive instructions (*skipping fault*).

At the end of the computation the attacker can read the result returned by the algorithm.

Remark 1. This fault injection model implies that faults can be injected very accurately in timing (the resolution is the clock period), whereas the fault locality in space is poor (the attacker cannot target a specific bit). This models an attacker who is able to identify the sequence of operations by a simple side-channel analysis, but who has no knowledge of the chip internals. Such attack model is realistic for designs where the memories are scrambled and the logic gates randomly routed (in a sea of gates).

Lemma 1. *The effect of a skipping fault (i.e., fault on the code) can be captured by considering only randomizing and zeroing faults (i.e., fault on the data).*

Proof. Indeed, if the skipped instructions are part of an arithmetic operation:

- either the computation has not been done at all and the value in memory where the result is supposed to be stays zero (if initialized) or random (if not),
- or the computation has partly been done and the value written in memory as its result is thus pseudo-randomized (and considered random at our modeling level).

If the skipped instruction is a branching instruction, then it is equivalent to do a zeroing fault on the result of the branching condition to make it false and thus avoid branching. □

Definition 2 (Attack order)**.** We call *order* of the attack the number of fault injections in the computation. An attack is said to be *high-order* if its order is strictly more than 1.

3 Classifying Countermeasures

The goal of a countermeasure against fault-injection attacks is to avoid returning a compromised value to the attacker. To this end, countermeasures attempt to verify the integrity of the computation before returning its result. If the integrity is compromised, then the returned value should be a random number or an error constant, in order not to leak any information.

An obvious way of achieving that goal is to repeat the computation and compare the results, but this approach is very expensive in terms of computation time. The same remark applies to the verification of the signature (notice that e can be recovered for this purpose from the 5-tuple (p, q, d_p, d_q, i_q), as explained in App. A). In this section we explore the different methods used by the existing countermeasures to verify the computation integrity faster than $(M^d)^e \stackrel{?}{\equiv} M \mod N$.

3.1 Shamir's or Giraud's Family of Countermeasures

To the authors knowledge, there are two main families of countermeasures: those which are descendants of Shamir's countermeasure [**?**], and those which are descendants of Giraud's [**?**].

The countermeasures in Giraud's family avoid replicating the computations using particular exponentiation algorithms. These algorithms keep track of variables involved in intermediate steps; those help verifying the consistency of the final results by a consistency check of an invariant that

is supposed to be spread till the last steps. This idea is illustrated in Alg. 2, which resembles the one of Giraud. The test at line 5 verifies that the recombined values S and S' (recombination of intermediate steps of the exponentiation) are consistent. Example of other countermeasures in this family are the ones of Boscher *et al.* [**?**], Rivain [**?**] (and its recently improved version [**?**]), or Kim *et al.* [**?**]. The former two mainly optimize Giraud's, while the latter introduce an infective verification based on binary masks. The detailed study of the countermeasures in Giraud's family is left as future work.

Algorithm 2: CRT-RSA with a Giraud's family countermeasure

Input : Message M, key (p, q, d_p, d_q, i_q)
Output: Signature $M^d \mod N$, or error

1 $(S_p, S'_p) = \mathsf{ExpAlgorithm}(M, d_p)$ `// ExpAlgorithm(a,b) returns` (a^b, a^{b-1})
2 $(S_q, S'_q) = \mathsf{ExpAlgorithm}(M, d_q)$
3 $S = S_q + q \cdot (i_q \cdot (S_p - S_q) \mod p)$ `// Recombination`
4 $S' = S'_q + q \cdot (i_q \cdot (S'_p - S'_q) \mod p)$ `// Recombination for verification`
5 **if** $M \cdot S' \not\equiv S \mod pq$ **then return** error
6 **return** S

Indeed, the rest of our paper is mainly concerned with Shamir's family of countermeasures. The countermeasures in Shamir's family rely on a kind of "checksum" of the computation using smaller numbers (the checksum is computed in rings smaller than the ones of the actual computation). The base-two logarithm of the smaller rings cardinal is typically equal to 32 or to 64 (bits): therefore, assuming that the faults are randomly distributed, the probability of having an undetected fault is 2^{-32} or 2^{-64}, *i.e.*, very low. In the sequel, we will make a language abuse by considering that such probability is equal to zero. We also use the following terminology:

Notation 1. *Let a a big number and b a small number, such that they are coprime. We call the ring $\mathbb{Z}_{ab}$ an* overring *of $\mathbb{Z}_a$, and the ring $\mathbb{Z}_b$ a* subring *of $\mathbb{Z}_{ab}$.*

Remark 2. RSA is friendly to protections by checksums because it computes in rings $\mathbb{Z}_a$ where a is either a large prime number (*e.g.*, $a = p$ or $a = q$) or the product of large prime numbers (*e.g.*, $a = p \cdot q$). Thus, any small number $b > 1$ is coprime with a, and so we have an isomorphism between the *overring* $\mathbb{Z}_{ab}$ and the direct product of $\mathbb{Z}_a$ and $\mathbb{Z}_b$, *i.e.*, $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$. This means that the Chinese Remainder Theorem applies. Consequently, the nominal computation and the checksum can be conducted in parallel in $\mathbb{Z}_{ab}$.

The countermeasures attempt to assert that some invariants on the computations and the checksums hold. There are many different ways to use the checksums and to verify these invariants. In the rest of this section we review these ways while we attempt to classify countermeasures and understand better what are the necessary invariants to verify.

3.2 Test-Based or Infective

A first way to classify countermeasures is to separate those which consist in step-wise internal checks during the CRT computation and those which use an infective computation strategy to make the result unusable by the attacker in case of fault injection.

Definition 3 (Test-based countermeasure)**.** A countermeasure is said to be *test-based* if it attempts to detect fault injections by verifying that some arithmetic invariants are respected, and branch to return an error instead of the numerical result of the algorithm in case of invariant violation. Examples of test-based countermeasures are the ones of Shamir [**?**], Aumüller *et al.* [**?**], Vigilant [**?**], or Joye *et al.* [**?**].

Definition 4 (Infective countermeasure)**.** A countermeasure is said to be *infective* if rather than testing arithmetic invariants it uses them to compute a neutral element of some arithmetic operation in a way that would not result in this neutral element if the invariant is violated. It then uses the results of these computations to infect the result of the algorithm before returning it to make it unusable by the attacker (thus, it does not need branching instructions). Examples of infective countermeasures are the ones by Blömer *et al.* [**?**], Ciet & Joye [**?**], or Kim *et al.* [**?**].

The extreme similarity between the verifications in the test-based countermeasure of Joye *et al.* [**?**] (see Alg. 3, line 9) and the infective countermeasure of Ciet & Joye [**?**] (see Alg. 4, lines 10 and 11) is striking, but it is actually not surprising at all, as we will discover in Prop. 2.

Algorithm 3: CRT-RSA with Joye *et al.*'s countermeasure [**?**]

Input : Message M, key (p, q, d_p, d_q, i_q)
Output: Signature $M^d \mod N$, or error

1 Choose two small random integers r_1 and r_2.
2 Store in memory $p' = p \cdot r_1$, $q' = q \cdot r_2$, $i'_q = q'^{-1} \mod p'$, $N = p \cdot q$.
3 $S'_p = M^{d_p \mod \varphi(p')} \mod p'$ // Intermediate signature in $\mathbb{Z}_{pr_1}$
4 $S_{pr} = M^{d_p \mod \varphi(r_1)} \mod r_1$ // Checksum in $\mathbb{Z}_{r_1}$
5 $S'_q = M^{d_q \mod \varphi(q')} \mod q'$ // Intermediate signature in $\mathbb{Z}_{qr_2}$
6 $S_{qr} = M^{d_q \mod \varphi(r_2)} \mod r_2$ // Checksum in $\mathbb{Z}_{r_2}$
7 $S_p = S'_p \mod p$ // Retrieve intermediate signature in $\mathbb{Z}_p$
8 $S_q = S'_q \mod q$ // Retrieve intermediate signature in $\mathbb{Z}_q$
9 **if** $S'_p \not\equiv S_{pr} \mod r_1$ **or** $S'_q \not\equiv S_{qr} \mod r_2$ **then return** error
10 **return** $S = S_q + q \cdot (i_q \cdot (S_p - S_q) \mod p)$ // Recombination in $\mathbb{Z}_N$

Proposition 2 (Equivalence between test-based and infective countermeasures)**.** *Each test-based (resp. infective) countermeasure has a direct equivalent infective (resp. test-based) countermeasure.*

Proof. The invariants that must be verified by countermeasures are modular equality, so they are of the form $a \stackrel{?}{\equiv} b \mod m$, where a, b and m are arithmetic expressions.

It is straightforward to transform this invariant into a Boolean expression usable in test-based countermeasures: `if a != b [mod m] then return` *error*.

To use it in infective countermeasures, it is as easy to verify the same invariant by computing a value which should be 1 if the invariant holds: `c := a - b + 1 mod m`. The numbers obtained this way for each invariant can then be multiplied and their product c^*, which is 1 only if all invariants are respected, can be used as an exponent on the algorithm's result to infect it if one or more of the tested invariants are violated. Indeed, when the attacker perform the BellCoRe attack by computing $\gcd(N, S - \widehat{S^{c^*}})$ as defined in Prop. 1, then if c^* is not 1 the attack would not work. □

Algorithm 4: CRT-RSA with Ciet & Joye's countermeasure [?]

Input : Message M, key (p, q, d_p, d_q, i_q)
Output: Signature $M^d \mod N$, or a random value in $\mathbb{Z}_N$

Choose small random integers r_1, r_2, and r_3.
Choose a random integer a.
Initialize γ with a random number
Store in memory $p' = p \cdot r_1$, $q' = q \cdot r_2$, $i'_q = q'^{-1} \mod p'$, $N = p \cdot q$.
$S'_p = a + M^{d_p \mod \varphi(p')} \mod p'$ // Intermediate signature in $\mathbb{Z}_{pr_1}$
$S_{pr} = a + M^{d_p \mod \varphi(r_1)} \mod r_1$ // Checksum in $\mathbb{Z}_{r_1}$
$S'_q = a + M^{d_q \mod \varphi(q')} \mod q'$ // Intermediate signature in $\mathbb{Z}_{qr_2}$
$S_{qr} = a + M^{d_q \mod \varphi(r_2)} \mod r_2$ // Checksum in $\mathbb{Z}_{r_2}$
$S' = S'_q + q' \cdot (i'_q \cdot (S'_p - S'_q) \mod p')$ // Recombination in $\mathbb{Z}_{Nr_1r_2}$
$c_1 = S' - S_{pr} + 1 \mod r_1$ // Invariant for the signature modulo p
$c_2 = S' - S_{qr} + 1 \mod r_2$ // Invariant for the signature modulo q
$\gamma = (r_3 \cdot c_1 + (2^l - r_3) \cdot c_2)/2^l$ // $\gamma = 1$ if c_1 and c_2 have value 1
return $S = S' - a^\gamma \mod N$ // Infection and result retrieval in $\mathbb{Z}_N$

By Prop. 2, we know that there is an equivalence between test-based and infective countermeasures. This means that in theory any attack working on one kind of countermeasure will be possible on the equivalent countermeasure of the other kind. However, we remark that in practice it is harder to do a zeroing fault on an intermediate value (especially if it is the result of a computation with big numbers) in the case of an infective countermeasure, than it is to skip one branching instruction in the case of a test-based countermeasure. We conclude from this the following rule of thumb: *it is better to use the infective variant of a countermeasure.* In addition, it is generally the case that code without branches is safer (think of timing attacks or branch predictor attacks on modern CPUs).

Note that if a fault occurs, c^* is not 1 anymore and thus the computation time required to compute S^{c^*} might significantly increase. This is not a security problem, indeed, taking longer to return a randomized value in case of an attack is not different from rapidly returning an error constant without finishing the computation first as it is done in the existing test-based countermeasures. In the worst case scenario, the additional time would be correlated to the induced fault, but we assume the fault to be controlled by the attacker already.

3.3 Intended Order

Countermeasures can be classified depending on their order, *i.e.*, the maximum order of the attacks (as per Def. 2) that they can protect against.

In the literature concerning CRT-RSA countermeasures against fault-injection attacks, most countermeasures claim to be first-order, and a few claim second-order resistance. For instance, the countermeasures by Aumüller *et al.* [?] and the one by Vigilant [?] are described as first-order by their authors, while Ciet & Joye [?] describe a second-order fault model and propose a countermeasure which is supposed to resist to this fault model, and thus be second-order.

However, using the finja[3] tool which has been open-sourced by Rauzy & Guilley [**?**], we found out that the countermeasure of Ciet & Joye is in fact vulnerable to second-order attacks (in our fault model of Def. 1). This is not very surprising. Indeed, Prop. 2 proves that injecting a fault, and then skipping the invariant verification which was supposed to catch the first fault injection, is a second-order attack strategy which also works for infective countermeasures, except the branching-instruction skip has to be replaced by a zeroing fault. As expected, the attacks we found using finja did exactly that. For instance a zeroing fault on S'_p (resp. S'_q) makes the computation vulnerable to the BellCoRe attack, and a following zeroing fault on S_{pr} (resp. S_{qr}) makes the verification pass anyway. To our knowledge our attack is new. It is indeed different from the one Dottax *et al.* [**?**] found and fixed in their paper, which was an attack on the use of γ (see line 12 of Alg. 4). It is true that their attack model only allows skipping faults (as per Def. 1) for the second injection, but we have concerns about this:

- What justifies this limitation on the second fault? Surely if the attackers are able to inject two faults and can inject a zeroing fault once they can do it twice.
- Even considering their attack model, a zeroing fault on an intermediate variable x can in many cases be obtained by skipping the instructions where the writing to x happens.
- The fixed version of the countermeasure by Dottax *et al.* [**?**, Alg. 8, p. 13] makes it even closer to the one of Joye *et al.* by removing the use of a and γ. It also removes the result infection part and instead returns S along with values that should be equal if no faults were injected, leaving "out" of the algorithm the necessary comparison and branching instructions which are presented in a separate procedure [**?**, Proc. 1, p. 11]. The resulting countermeasure is second-order resistant (in their attack model) only because the separate procedure does the necessary tests twice (it would indeed break at third-order unless an additional repetition of the test is added, *etc.*).

An additional remark would be that the algorithms of intended second-order countermeasures does not look very different from others. Moreover, Rauzy & Guilley [**?**, **?**] exposed evidence that the intendedly first-order countermeasures of Aumüller *et al.* and Vigilant actually offer the same level of resistance against second-order attacks, *i.e.*, they resist when the second injected fault is a randomizing fault (or a skipping fault which amounts to a randomizing fault).

3.4 Usage of the Small Rings

In most countermeasures, the computation of the two intermediate signatures modulo p and modulo q of the CRT actually takes place in overrings. The computation of S_p (resp. S_q) is done in $\mathbb{Z}_{pr_1}$ (resp. $\mathbb{Z}_{qr_2}$) for some small random number r_1 (resp. r_2) rather than in $\mathbb{Z}_p$ (resp. $\mathbb{Z}_q$). This allows the retrieval of the results by reducing modulo p (resp. q) and verifying the signature modulo r_1 (resp. r_2), or, if it is done after the CRT recombination, the results can be retrieved by reducing modulo $N = p \cdot q$. The reduction in the *small subrings* $\mathbb{Z}_{r_1}$ and $\mathbb{Z}_{r_2}$ is used as the checksums for verifying the integrity of the computation. It works because small random numbers are necessarily coprime with a big prime number.

An interesting part of countermeasures is how they use the small subrings to verify the integrity of the computations. Almost all the various countermeasures we studied had different ways of using them. However, they can be divided in two groups. On one side there are countermeasures which use the small subrings to verify the integrity of the intermediate CRT signatures and of

[3] `http://pablo.rauzy.name/sensi/finja.html` (we used the commit `782384a` version of the code).

the recombination directly but using smaller numbers, like Blömer *et al.*'s countermeasure [**?**], or Ciet & Joye's one [**?**]. On the other side, there are countermeasures which use some additional arithmetic properties to verify the necessary invariants indirectly in the small subrings. Contrary to the countermeasures in the first group, the ones in the second group use the same value r for r_1 and r_2. The symmetry obtained with $r_1 = r_2$ is what makes the additional arithmetic properties hold, as we will see.

3.4.1 Verification of the Intermediate CRT Signatures

The countermeasure of Blömer *et al.* [**?**] uses the small subrings to verify the intermediate CRT signatures. It is exposed in Alg. 5. This countermeasure needs access to d directly rather than d_p and d_q as the standard interface for CRT-RSA suggests, in order to compute $d'_p = d \mod \varphi(p \cdot r_1)$ and $d'_q = d \mod \varphi(q \cdot r_2)$, as well as their inverse $e'_p = {d'_p}^{-1} \mod \varphi(p \cdot r_1)$ and $e'_q = {d'_q}^{-1} \mod \varphi(q \cdot r_2)$ to verify the intermediate CRT signatures.

We can see in Alg. 5 that these verifications (lines 6 and 7) happen after the recombination (line 5) and retrieve the checksums in $\mathbb{Z}_{r_1}$ (for the p part of the CRT) and $\mathbb{Z}_{r_2}$ (for the q part) from the recombined value S'. It allows these tests to verify the integrity of the recombination at the same time as they verify the integrity of the intermediate CRT signatures.

Algorithm 5: CRT-RSA with Blömer *et al.*'s countermeasure [**?**]

Input : Message M, key (p, q, d, i_q)
Output: Signature $M^d \mod N$, or a random value in $\mathbb{Z}_N$

1 Choose two small random integers r_1 and r_2.
2 Store in memory $p' = p \cdot r_1$, $q' = q \cdot r_2$, $i'_q = {q'}^{-1} \mod p'$, $N = p \cdot q$, $N' = N \cdot r_1 \cdot r_2$, d'_p, d'_q, e'_p, e'_q.
3 $S'_p = M^{d'_p} \mod p'$ // Intermediate signature in $\mathbb{Z}_{pr_1}$
4 $S'_q = M^{d'_q} \mod q'$ // Intermediate signature in $\mathbb{Z}_{qr_2}$
5 $S' = S'_q + q' \cdot (i'_q \cdot (S'_p - S'_q) \mod p')$ // Recombination in $\mathbb{Z}_{Nr_1r_2}$
6 $c_1 = M - {S'}^{e'_p} + 1 \mod r_1$ // Invariant for the signature modulo p
7 $c_2 = M - {S'}^{e'_q} + 1 \mod r_2$ // Invariant for the signature modulo q
8 **return** $S = {S'}^{c_1 c_2} \mod N$ // Infection and result retrieval in $\mathbb{Z}_N$

3.4.2 Checksums of the Intermediate CRT Signatures

The countermeasure of Ciet & Joye [**?**] uses the small subrings to compute checksums of the intermediate CRT signatures. It is exposed in Alg. 4. Just as the previous one, the verifications (lines 10 and 11) take place after the recombination (line 9) and retrieve the checksums in $\mathbb{Z}_{r_1}$ (for the p part of the CRT) and $\mathbb{Z}_{r_2}$ (for the q part) from the recombined value S', which enables the integrity verification of the recombination at the same time as the integrity verifications of the intermediate CRT signatures.

We note that this is missing from the protection of Joye *et al.* [**?**], presented in Alg. 3, which does not verify the integrity of the recombination at all and is thus as broken as Shamir's countermeasure [**?**]. The countermeasure of Ciet & Joye is a clever fix against the possible fault attacks

on the recombination of Joye *et al.*'s countermeasure, which also uses the transformation that we described in Prop. 2 from a test-based to an infective countermeasure.

3.4.3 Overrings for CRT Recombination

In Ciet & Joye's countermeasure the CRT recombination happens in an overring $\mathbb{Z}_{Nr_1r_2}$ of $\mathbb{Z}_N$ while Joye *et al.*'s countermeasure extracts in $\mathbb{Z}_p$ and $\mathbb{Z}_q$ the results S_p and S_q of the intermediate CRT signatures to do the recombination in $\mathbb{Z}_N$ directly.

There are only two other countermeasures which do the recombination in $\mathbb{Z}_N$ that we know of: the one of Shamir [**?**] and the one of Aumüller *et al.* [**?**]. The first one is known to be broken, in particular because it does not check whether the recombination has been faulted at all. The second one seems to need to verify 5 invariants to resist the BellCoRe attack[4], which is more than the only 2 required by the countermeasure of Ciet & Joye [**?**] or by the one of Blömer *et al.* [**?**], while offering a similar level of protection (see [**?**]). This fact led us to think that the additional tests are necessary because the recombination takes place "in the clear". But we did not jump right away to that conclusion. Indeed, Vigilant's countermeasure [**?**] does the CRT recombination in the $\mathbb{Z}_{Nr^2}$ overring of $\mathbb{Z}_N$ and seems to require 7 verifications[5] to also offer that same level of security (see [**?**]). However, we remark that Shamir's, Aumüller *et al.*'s, and Vigilant's countermeasures use the same value for r_1 and r_2.

3.4.4 Identity of r_1 and r_2

Some countermeasures, such as the ones of Shamir [**?**], Aumüller *et al.* [**?**], and Vigilant [**?**] use a single random number r to construct the overrings used for the two intermediate CRT signatures computation. The resulting symmetry allows these countermeasures to take advantage of some additional arithmetic properties.

Shamir's countermeasure In his countermeasure, which is presented in Alg. 6, Shamir uses a clever invariant property to verify the integrity of both intermediate CRT signatures in a single verification step (line 9). This is made possible by the fact that he uses d directly instead of d_p and d_q, and thus the checksums in $\mathbb{Z}_r$ of both the intermediate CRT signatures are supposed to be equal if no fault occurred. Unfortunately, the integrity of the recombination is not verified at all. We will see in Sec. 5.1 how to fix this omission. Besides, we notice that d can be reconstructed from a usual CRT-RSA key (p, q, d_p, d_q, i_q); we refer the reader to Appendix A.

Aumüller *et al.*'s countermeasure Contrary to Shamir, Aumüller *et al.* do verify the integrity of the recombination in their countermeasure, which is presented in Alg. 7. To do this, they straightforwardly check (line 10) that when reducing the result S of the recombination modulo p (resp. q), the obtained value corresponds to the intermediate signature in $\mathbb{Z}_p$ (resp. $\mathbb{Z}_q$). However, they do not use d directly but rather conform to the standard CRT-RSA interface by using d_p and d_q. Thus, they need another verification to check the integrity of the intermediate CRT signatures. Their clever strategy is to verify that the checksums of S_p and S_q in $\mathbb{Z}_r$ are conform to each other

[4]The original Aumüller *et al.*'s countermeasure uses 7 verifications because it also needs to check the integrity of intermediate values introduced against simple power analysis, see [**?**, Remark 1].

[5]Vigilant's original countermeasure and its corrected version by Coron *et al.* [**?**] actually use 9 verifications but were simplified by Rauzy & Guilley [**?**] who removed 2 verifications.

Algorithm 6: CRT-RSA with Shamir's countermeasure [?]

Input : Message M, key (p, q, d, i_q)
Output: Signature $M^d \mod N$, or error

1 Choose a small random integer r.
2 $p' = p \cdot r$
3 $S'_p = M^{d \mod \varphi(p')} \mod p'$ // Intermediate signature in $\mathbb{Z}_{pr}$
4 $q' = q \cdot r$
5 $S'_q = M^{d \mod \varphi(q')} \mod q'$ // Intermediate signature in $\mathbb{Z}_{qr}$
6 $S_p = S'_p \mod p$ // Retrieve intermediate signature in $\mathbb{Z}_p$
7 $S_q = S'_q \mod q$ // Retrieve intermediate signature in $\mathbb{Z}_q$
8 $S = S_q + q \cdot (i_q \cdot (S_p - S_q) \mod p)$ // Recombination in $\mathbb{Z}_N$
9 **if** $S'_p \not\equiv S'_q \mod r$ **then return** error
10 **return** S

(lines 11 to 13). For that they check whether ${S_p}^{d_q}$ is equal to ${S_q}^{d_p}$ in $\mathbb{Z}_r$, that is, whether the invariant $(M^{d_p})^{d_q} \equiv (M^{d_q})^{d_p} \mod r$ holds.

The two additional tests on line 4 verify the integrity of p' and q'. Indeed, if p or q happen to be randomized when computing p' or q' the invariant verifications in $\mathbb{Z}_r$ would pass but the retrieval of the intermediate signatures in $\mathbb{Z}_p$ or $\mathbb{Z}_q$ would return random values, which would make the BellCoRe attack work. These important verifications are missing from all the previous countermeasures in Shamir's family.

Vigilant's countermeasure Vigilant takes another approach. Rather than doing the integrity verifications on "direct checksums" that are the representative values of the CRT-RSA computation in the small subrings, Vigilant uses different values that he constructs for that purpose. The clever idea of his countermeasure is to use sub-CRTs on the values that the CRT-RSA algorithm manipulates in order to have in one part the value we are interested in and in the other the value constructed for the verification (lines 8 and 17).

To do this, he transforms M into another value M' such that:

$$M' \equiv \begin{cases} M & \mod N, \\ 1 + r & \mod r^2, \end{cases}$$

which implies that:

$$S' = M'^d \mod Nr^2 \equiv \begin{cases} M^d & \mod N, \\ 1 + dr & \mod r^2. \end{cases}$$

The latter results are based on the binomial theorem, which states that $(1 + r)^d = \sum_{k=0}^{d} \binom{d}{k} r^k = 1 + dr + \binom{d}{2} r^2 + \ldots$, which simplifies to $1 + dr$ in the $\mathbb{Z}_{r^2}$ ring.

This property is used to verify the integrity of the intermediate CRT signatures on lines 11 and 20. It is also used on line 24 which tests the recombination using the same technique but with random values inserted on lines 21 and 22 in place of the constructed ones. This test also verifies the integrity of N.

Algorithm 7: CRT-RSA with Aumüller *et al.*'s countermeasure[6] [**?**]

Input : Message M, key (p, q, d_p, d_q, i_q)
Output: Signature $M^d \mod N$, or error

1 Choose a small random integer r.
2 $p' = p \cdot r$
3 $q' = q \cdot r$
4 **if** $p' \not\equiv 0 \mod p$ **or** $q' \not\equiv 0 \mod q$ **then return** error
5 $S'_p = M^{d_p \mod \varphi(p')} \mod p'$ // Intermediate signature in $\mathbb{Z}_{pr}$
6 $S'_q = M^{d_q \mod \varphi(q')} \mod q'$ // Intermediate signature in $\mathbb{Z}_{qr}$
7 $S_p = S'_p \mod p$ // Retrieve intermediate signature in $\mathbb{Z}_p$
8 $S_q = S'_q \mod q$ // Retrieve intermediate signature in $\mathbb{Z}_q$
9 $S = S_q + q \cdot (i_q \cdot (S_p - S_q) \mod p)$ // Recombination in $\mathbb{Z}_N$
10 **if** $S \not\equiv S'_p \mod p$ **or** $S \not\equiv S'_q \mod q$ **then return** error
11 $S_{pr} = S'_p \mod r$ // Checksum of S_p in $\mathbb{Z}_r$
12 $S_{qr} = S'_q \mod r$ // Checksum of S_q in $\mathbb{Z}_r$
13 **if** ${S_{pr}}^{d_q \mod \varphi(r)} \not\equiv {S_{qr}}^{d_p \mod \varphi(r)} \mod r$ **then return** error
14 **return** S

Two additional tests are required by Vigilant's arithmetic trick. The verifications at lines 10 and 19 ensure that the original message M has indeed been CRT-embedded in M'_p and M'_q.

4 The Essence of a Countermeasure

Our attempt to classify the existing countermeasures provided us with a deep understanding of how they work. To ensure the integrity of the CRT-RSA computation, the algorithm must verify 3 things: the integrity of the computation modulo p, the integrity of the computation modulo q, and the integrity of the CRT recombination (which can be subject to transient fault attacks). This fact has been known since the first attacks on Shamir's countermeasure. Our study of the existing countermeasures revealed that, as expected, those which perform these three integrity verifications are the ones which actually work. This applies to Shamir's family of countermeasures, but also for Giraud's family. Indeed, countermeasures in the latter also verify the two exponentiations and the recombination by testing the consistency of the exponentiations indirectly on the recombined value.

4.1 A Straightforward Countermeasure

The result of these observations is a very straightforward countermeasure, presented in Alg. 9. This countermeasure works by testing the integrity of the signatures modulo p and q by replicating the computations (lines 1 and 3) and comparing the results, and the integrity of the recombination by verifying that the two parts of the CRT can be retrieved from the final result (line 5). This

[6] For the sake of simplicity we removed some code that served against SPA (simple power analysis) and only kept the necessary code against fault-injection attacks.

Algorithm 8: CRT-RSA with Vigilant's countermeasure[6] [?]

with Coron *et al.*'s fixes [?] and Rauzy & Guilley's simplifications [?]

Input : Message M, key (p, q, d_p, d_q, i_q)
Output: Signature $M^d \mod N$, or error

1 Choose small random integers r, R_1, and R_2.
2 $N = p \cdot q$
3 $p' = p \cdot r^2$
4 $i_{pr} = p^{-1} \mod r^2$
5 $M_p = M \mod p'$
6 $B_p = p \cdot i_{pr}$
7 $A_p = 1 - B_p \mod p'$
8 $M'_p = A_p \cdot M_p + B_p \cdot (1 + r) \mod p'$ // CRT insertion of verification value in M'_p
9 $S'_p = M'^{d_p \mod \varphi(p')}_p \mod p'$ // Intermediate signature in $\mathbb{Z}_{pr^2}$
10 **if** $M'_p \not\equiv M \mod p$ **then return** error
11 **if** $B_p \cdot S'_p \not\equiv B_p \cdot (1 + d_p \cdot r) \mod p'$ **then return** error
12 $q' = q \cdot r^2$
13 $i_{qr} = q^{-1} \mod r^2$
14 $M_q = M \mod q'$
15 $B_q = q \cdot i_{qr}$
16 $A_q = 1 - B_q \mod q'$
17 $M'_q = A_q \cdot M_q + B_q \cdot (1 + r) \mod q'$ // CRT insertion of verification value in M'_q
18 $S'_q = M'^{d_q \mod \varphi(q')}_q \mod q'$ // Intermediate signature in $\mathbb{Z}_{qr^2}$
19 **if** $M'_q \not\equiv M \mod q$ **then return** error
20 **if** $B_q \cdot S'_q \not\equiv B_q \cdot (1 + d_q \cdot r) \mod q'$ **then return** error
21 $S_{pr} = S'_p - B_p \cdot (1 + d_p \cdot r - R_1)$ // Verification value of S'_p swapped with R_1
22 $S_{qr} = S'_q - B_q \cdot (1 + d_q \cdot r - R_2)$ // Verification value of S'_q swapped with R_2
23 $S_r = S_{qr} + q \cdot (i_q \cdot (S_{pr} - S_{qr}) \mod p')$ // Recombination in $\mathbb{Z}_{Nr^2}$
// Simultaneous verification of lines 2 and 23
24 **if** $pq \cdot (S_r - R_2 - q \cdot i_q \cdot (R_1 - R_2)) \not\equiv 0 \mod Nr^2$ **then return** error
25 **return** $S = S_r \mod N$ // Retrieve result in $\mathbb{Z}_N$

countermeasure is of course very expensive since the two big exponentiations are done twice, and is thus not usable in practice. Note that it is nonetheless still better in terms of speed than computing RSA without the CRT optimization.

Algorithm 9: CRT-RSA with straightforward countermeasure

Input : Message M, key (p, q, d_p, d_q, i_q)
Output: Signature $M^d \mod N$, or error

1 $S_p = M^{d_p \mod \varphi(p)} \mod p$ // Intermediate signature in $\mathbb{Z}_p$
2 **if** $S_p \not\equiv M^{d_p} \mod p$ **then return** error
3 $S_q = M^{d_q \mod \varphi(q)} \mod q$ // Intermediate signature in $\mathbb{Z}_q$
4 **if** $S_q \not\equiv M^{d_q} \mod q$ **then return** error
5 $S = S_q + q \cdot (i_q \cdot (S_p - S_q) \mod p)$ // Recombination in $\mathbb{Z}_N$
6 **if** $S \not\equiv S_p \mod p$ **or** $S \not\equiv S_q \mod q$ **then return** error
7 **return** S

Proposition 3 (Correctness)**.** *The straightforward countermeasure (and thus all the ones which do equivalent verifications) is secure against first-order fault attacks as per Def. 1 and 2.*

Proof. The proof is in two steps. First, prove that if the intermediate signatures are not correct, then the tests at lines 2 and 4 returns error. Second, prove that if both tests passed then either the recombination is correct or the test at line 6 returns error.

If a fault occurs during the computation of S_p (line 1), then it either has the effect of zeroing its value or randomizing it, as shown by Lem. 1. Thus, the test of line 2 detects it since the two compared values won't be equal. If the fault happens on line 2, then either we are in a symmetrical case: the repeated computation is faulted, or the test is skipped: in that case there are no faults affecting the data so the test is unnecessary anyway. It works similarly for the intermediate signature in $\mathbb{Z}_q$.

If the first two tests pass, then the tests at line 6 verify that both parts of the CRT computation are indeed correctly recombined in S. If a fault occurs during the recombination on line 5 it will thus be detected. If the fault happens at line 6, then either it is a fault on the data and one of the two tests returns error, or it is a skipping fault which bypasses one or both tests but in that case there are no faults affecting the data so the tests are unnecessary anyway. □

4.2 High-Order Countermeasures

Using the finja[3] tool we were able to verify that removing one of the three integrity checks indeed breaks the countermeasure against first-order attacks. Nonetheless, each countermeasure which has these three integrity checks, plus those that may be necessary to protect optimizations on them, offers the same level of protection.

Proposition 4 (High-order countermeasures)**.** *Against randomizing faults, all correct countermeasures (as per Prop. 3) are high-order. However, there are no generic high-order countermeasures if the three types of faults in our attack model are taken into account, but it is possible to build nth-order countermeasures for any n.*

Proof. Indeed, if a countermeasure is able to detect a single randomizing fault, then adding more faults will not break the countermeasure, since a random fault cannot induce a verification skip. Thus, *all working countermeasures are high-order against randomizing faults.*

However, if after one or more faults which permit an attack, there is a skipping fault or a zeroing fault which leads to skip the verification which would detect the previous fault injections, then the attack will work. As Lem. 1 and Prop. 2 explain, this is true for all countermeasures, not only those which are test-based but also the infective ones. It seems that the only way to protect against that is to replicate of the integrity checks. If each invariant is verified n times, then the countermeasure will resist at least n faults in the worst case scenario: a single fault is used to break the computation and the n others to avoid the verifications which detect the effect of the first fault. Thus, *there are no generic high-order countermeasures* if the three types of faults in our attack model are taken into account, ***but it is possible to build a*** n**th*-order countermeasure for any*** n **by replicating the invariant verifications** n **times**. □

Existing first-order countermeasures such as the ones of Aumüller *et al.* (Alg. 7, 13), Vigilant (Alg. 8, 11), or Ciet & Joye (Alg. 4) can thus be transformed into nth-order countermeasures, in the attack model described in Def. 1 and 2. As explained, the transformation consists in replicating the verifications n times, whether they are test-based or infective.

This result means that it is very important that the verifications be cost effective. Fortunately, as we saw in Sec. 3 and particularly in Sec. 3.4 on the usage of the small rings, the existing countermeasures offer exactly that: optimized versions of Alg. 9 that use a variety of invariant properties to avoid replicating the two big exponentiations of the CRT computation.

5 Building Better or Different Countermeasures

In the two previous sections we learned a lot about current countermeasures and how they work. We saw that to reduce their cost, most countermeasures use invariant properties to optimize the verification speed by using checksums on smaller numbers than the big ones which are manipulated by the protected algorithm. Doing so, we understood how these optimizations work and the power of their underlying ideas. In this section apply our newly acquired knowledge on the *essence of countermeasures* in order to build the *quintessence of countermeasures*. Namely, we leverage our findings to fix Shamir's countermeasure, and to drastically simplify the one of Vigilant, while at the same time transforming it to be infective instead of test-based.

5.1 Correcting Shamir's Countermeasure

We saw that Shamir's countermeasure is broken in multiple ways, which has been known for a long time now. To fix it without denaturing it, we need to verify the integrity of the recombination as well as the ones of the overrings moduli. We can directly take these verifications from Aumüller *et al.*'s countermeasure. The result can be observed in Alg. 10.

The additional tests on line 4 protect against transient faults on p (resp. q) while computing p' (resp. q'), which would amount to a randomization of S'_p (resp. S'_q) while computing the intermediate signatures. The additional test on line 7 verifies the integrity of the intermediate signature computations.

Algorithm 10: CRT-RSA with a fixed version of Shamir's countermeasure
(new algorithm contributed in this paper)

Input : Message M, key (p, q, d, i_q)
Output: Signature $M^d \mod N$, or error

1 Choose a small random integer r.
2 $p' = p \cdot r$
3 $q' = q \cdot r$
4 **if** $p' \not\equiv 0 \mod p$ **or** $q' \not\equiv 0 \mod q$ **then return** error
5 $S'_p = M^{d \mod \varphi(p')} \mod p'$ // Intermediate signature in $\mathbb{Z}_{pr}$
6 $S'_q = M^{d \mod \varphi(q')} \mod q'$ // Intermediate signature in $\mathbb{Z}_{qr}$
7 **if** $S'_p \not\equiv S'_q \mod r$ **then return** error
8 $S_p = S'_p \mod p$ // Retrieve intermediate signature in $\mathbb{Z}_p$
9 $S_q = S'_q \mod q$ // Retrieve intermediate signature in $\mathbb{Z}_q$
10 $S = S_q + q \cdot (i_q \cdot (S_p - S_q) \mod p)$ // Recombination in $\mathbb{Z}_N$
11 **if** $S \not\equiv S'_p \mod p$ **or** $S \not\equiv S'_q \mod q$ **then return** error
12 **return** S

5.2 Simplifying Vigilant's Countermeasure

The mathematical tricks used in the Vigilant countermeasure are very powerful. Their understanding enabled the optimization of his countermeasure to only need 3 verifications, while the original version has 9. Our simplified version of the countermeasure can be seen in Alg. 11. Our idea is that it is not necessary to perform the checksum value replacements at lines 21 and 22 of Alg. 8 (see Sec. 3.4). What is more, if these replacements are not done, then the algorithm's computations carry the CRT-embedded checksum values until the end, and *the integrity of the whole computation can be tested with a single verification* in $\mathbb{Z}_{r^2}$ (line 23 of Alg. 11).

This idea not only reduces the number of required verifications, which is in itself a security improvement as shown in Sec. 3.2, but it also optimizes the countermeasure for speed and reduces its need for randomness (the computations of lines 21 and 22 of Alg. 8 are removed).

The two other tests that are left are the ones of lines 10 and 19 in Alg. 8, which ensure that the original message M has indeed been CRT-embedded in M'_p and M'_q. We take advantage of these two tests to verify the integrity of N both modulo p and modulo q (lines 17 and 20 of Alg. 11).

Remark 3. Note that we also made this version of the countermeasure infective, using the transformation method that we exposed in Sec. 3.2. As we said, any countermeasure can be transformed this way, for instance Alg. 13 in the Appendix B presents an infective variant of Aumüller *et al.*'s countermeasure.

6 Conclusions and Perspectives

We studied the existing CRT-RSA algorithm countermeasures against fault-injection attacks, in particular the ones of Shamir's family. In so doing, we got a deeper understanding of their ins and outs. We obtained a few intermediate results: the absence of conceptual distinction between

Algorithm 11: CRT-RSA with our simplified Vigilant's countermeasure, under its infective avatar (new algorithm contributed in this paper)

Input : Message M, key (p, q, d_p, d_q, i_q)
Output: Signature $M^d \mod N$, or a random value in $\mathbb{Z}_N$

Choose a small random integer r.
$N = p \cdot q$
$p' = p \cdot r^2$
$i_{pr} = p^{-1} \mod r^2$
$M_p = M \mod p'$
$B_p = p \cdot i_{pr}$
$A_p = 1 - B_p \mod p'$
$M'_p = A_p \cdot M_p + B_p \cdot (1 + r) \mod p'$ // CRT insertion of verification value in M'_p
$q' = q \cdot r^2$
$i_{qr} = q^{-1} \mod r^2$
$M_q = M \mod q'$
$B_q = q \cdot i_{qr}$
$A_q = 1 - B_q \mod q'$
$M'_q = A_q \cdot M_q + B_q \cdot (1 + r) \mod q'$ // CRT insertion of verification value in M'_q
$S'_p = {M'_p}^{d_p \mod \varphi(p')} \mod p'$ // Intermediate signature in $\mathbb{Z}_{pr^2}$
$S_{pr} = 1 + d_p \cdot r$ // Checksum in $\mathbb{Z}_{r^2}$ for S'_p
$c_p = M'_p + N - M + 1 \mod p$
$S'_q = {M'_q}^{d_q \mod \varphi(q')} \mod q'$ // Intermediate signature in $\mathbb{Z}_{qr^2}$
$S_{qr} = 1 + d_q \cdot r$ // Checksum in $\mathbb{Z}_{r^2}$ for S'_q
$c_q = M'_q + N - M + 1 \mod q$
$S' = S'_q + q \cdot (i_q \cdot (S'_p - S'_q) \mod p')$ // Recombination in $\mathbb{Z}_{Nr^2}$
$S_r = S_{qr} + q \cdot (i_q \cdot (S_{pr} - S_{qr}) \mod p')$ // Recombination checksum in $\mathbb{Z}_{r^2}$
$c_S = S' - S_r + 1 \mod r^2$
return $S = S'^{c_p c_q c_S} \mod N$ // Retrieve result in $\mathbb{Z}_N$

test-based and infective countermeasures, the fact that faults on the code (skipping instructions) can be captured by considering only faults on the data, and the fact that the many countermeasures that we studied (and their variations) were actually applying a common protection strategy but optimized it in different ways. These intermediate results allowed us to describe the design of a high-order countermeasure against our very generic fault model (comprised of randomizing, zeroing, and skipping faults). Our design allows to build a countermeasure resisting n faults for any n at a very reduced cost (it consists in adding $n-1$ comparisons on small numbers). We were also able to fix Shamir's countermeasure, and to drastically improve the one of Vigilant, going from 9 verifications in the original countermeasure to only 3, removing computations made useless, and reducing its need for randomness, while at the same time making it infective instead of test-based.

Except for those which rely on the fact that the protected algorithm takes the form of a CRT computation, the ideas presented in the various countermeasures can be applied to any modular arithmetic computation. For instance, it could be done using the idea of Vigilant consisting in using the CRT to embed a known subring value in the manipulated numbers to serve as a checksum. That would be the most obvious perspective for future work, as it would allow a generic approach against fault attacks and even automatic insertion of the countermeasure.

A study of Giraud's family of countermeasures in more detail would be beneficial to the community as well.

Acknowledgment

We would like to thank Antoine Amarilli for his proofreading which greatly improved the editorial quality of our manuscript.

References

A Recovering d and e from (p, q, d_p, d_q, i_q)

We prove here the following proposition:

Proposition 5. *It is possible to recover the private exponent d and the public exponent e from the 5-tuple (p, q, d_p, d_q, i_q) described in Sec. 2.2.*

Proof. Clearly, $p-1$ and $q-1$ are neither prime, nor coprimes (they have at least 2 as a common factor). Thus, proving Prop. 5 is not a trivial application of the Chinese Remainder Theorem. The proof we provide is elementary, but to our best knowledge, it has never been published before.

The numbers $p_1 = \frac{p-1}{\gcd(p-1,q-1)}$ and $q_1 = \frac{q-1}{\gcd(p-1,q-1)}$ are coprime, but there product is not equal to $\lambda(N)$. There is a factor $\gcd(p-1, q-1)$ missing, since $\lambda(N) = p_1 \cdot q_1 \cdot \gcd(p-1, q-1)$.

Now, $\gcd(p-1, q-1)$ is expected to be small. Thus, the following Alg. 12 can be applied efficiently. In this algorithm, the invariant is that p_2 and q_2, initially equal to p_1 and p_2, remain coprime. Moreover, they keep on increasing whereas r_2, initialized to $r_1 = \gcd(p-1, q-1)$, keeps on decreasing till 1.

Algorithm 12: Factorization of $\lambda(N)$ into two coprimes, multiples of p_1 and q_1 respectively.

Input : $p_1 = \frac{p-1}{\gcd(p-1,q-1)}$, $q_1 = \frac{q-1}{\gcd(p-1,q-1)}$ and $r_1 = \gcd(p-1, q-1)$
Output: (p_2, q_2), coprime, such as $p_2 \cdot q_2 = \lambda(N)$

$(p_2, q_2, r_2) \leftarrow (p_1, q_1, r_1)$
$g \leftarrow \gcd(p_2, r_2)$
while $g \neq 1$ **do**
  $p_2 \leftarrow p_2 \cdot g$
  $r_2 \leftarrow r_2/g$
  $g \leftarrow \gcd(p_2, r_2)$
end
$g \leftarrow \gcd(q_2, r_2)$
while $g \neq 1$ **do**
  $q_2 \leftarrow q_2 \cdot g$
  $r_2 \leftarrow r_2/g$
  $g \leftarrow \gcd(q_2, r_2)$
end
// p_2, q_2 and r_2 are now coprime
$q_2 \leftarrow q_2 \cdot r_2$ // $p_2 \leftarrow p_2 \cdot r_2$ would work equally
$(r_2 \leftarrow r_2/r_2 = 1)$ // For more pedagogy
return (p_2, q_2)

Let us denote p_2 and q_2 the two outputs of Alg. 12, we have:

- $d_{p_2} = d_p \mod p_2$, since $p_2|(p-1)$;
- $d_{q_2} = d_q \mod q_2$, since $q_2|(q-1)$;
- $i_{12} = {p_2}^{-1} \mod q_2$, since p_2 and q_2 are coprime.

We can apply Garner's formula to recover d:

$$d = d_{p_2} + p_2 \cdot ((i_{12} \cdot (d_{q_2} - d_{p_2})) \mod q_2) \ . \tag{1}$$

By Garner, we know that $0 \leq d < p_2 \cdot q_2 = \lambda(N)$, which is consistent with the remark made in the last sentence of Sec. 2.1.

Once we know the private exponent d, the public exponent e can be computed as the inverse of d modulo $\lambda(N)$. □

B Infective Aumüller CRT-RSA

The infective variant of Aumüller protection against CRT-RSA is detailed in Alg. 13.

Algorithm 13: CRT-RSA with Aumüller *et al.*'s countermeasure[6], under its infective avatar (new algorithm contributed in this paper)

Input : Message M, key (p, q, d_p, d_q, i_q)
Output: Signature $M^d \mod N$, or a random value

1 Choose a small random integer r.
2 $p' = p \cdot r$
3 $c_1 = p' + 1 \mod p$
4 $q' = q \cdot r$
5 $c_2 = q' + 1 \mod q$
6 $S'_p = M^{d_p \mod \varphi(p')} \mod p'$ // Intermediate signature in $\mathbb{Z}_{pr}$
7 $S'_q = M^{d_q \mod \varphi(q')} \mod q'$ // Intermediate signature in $\mathbb{Z}_{qr}$
8 $S_p = S'_p \mod p$ // Retrieve intermediate signature in $\mathbb{Z}_p$
9 $S_q = S'_q \mod q$ // Retrieve intermediate signature in $\mathbb{Z}_q$
10 $S = S_q + q \cdot (i_q \cdot (S_p - S_q) \mod p)$ // Recombination in $\mathbb{Z}_N$
11 $c_3 = S - S'_p + 1 \mod p$
12 $c_4 = S - S'_q + 1 \mod q$
13 $S_{pr} = S'_p \mod r$ // Checksum of S_p in $\mathbb{Z}_r$
14 $S_{qr} = S'_q \mod r$ // Checksum of S_q in $\mathbb{Z}_r$
15 $c_5 = {S_{pr}}^{d_q \mod \varphi(r)} - {S_{qr}}^{d_p \mod \varphi(r)} + 1 \mod r$
16 **return** $S^{c_1 c_2 c_3 c_4 c_5}$