On the Validity of the Φ-Hiding Assumption in Cryptographic Protocols

Christian Schridde and Bernd Freisleben

Department of Mathematics and Computer Science, University of Marburg
Hans-Meerwein-Str. 3, D-35032 Marburg, Germany
{schriddc,freisleb}@informatik.uni-marburg.de

Abstract. Most cryptographic protocols, in particular asymmetric protocols, are based on assumptions about the computational complexity of mathematical problems. The Φ-Hiding assumption is such an assumption. It states that if p_1 and p_2 are small primes exactly one of which divides $\varphi(N)$, where N is a number whose factorization is unknown and φ is Euler's totient function, then there is no polynomial-time algorithm to distinguish which of the primes p_1 and p_2 divides $\varphi(N)$ with a probability significantly greater than 1/2. In this paper, it will be shown that the Φ-Hiding assumption is not valid when applied to a modulus $N = PQ^{2e}$, where $P, Q > 2$ are primes, $e > 0$ is an integer and P hides the prime in question. This indicates that cryptographic protocols using such moduli and relying on the Φ-Hiding assumption must be handled with care.

Keywords: Φ-Hiding assumption, Jacobi symbol, Euler's totient function

1 Introduction

The Φ-Hiding assumption as defined by Cachin, Micali and Stadler [3] is an assumption about the difficulty of finding small factors of $\varphi(N)$, where N is a number whose factorization is unknown, and $\varphi(\cdot)$ is Euler's totient function, i.e. the number of positive integers less than or equal to N that are coprime to N. The security of several cryptosystems is based on the presumed difficulty of solving this problem [2, 5–7]. In this paper, it will be shown how information about the unknown factors of $\varphi(N)$ can be obtained when the modulus N is chosen as $N = PQ^{2e}$, where $P, Q > 2$ are primes, $e > 0$ is an integer and P hides the prime in question, such that the Φ-Hiding assumption is not valid in this case. Moduli of the form $N = PQ^{2e}$ are called *Multi-Power RSA* moduli and are used to speed up cryptographic operations [1]. In addition, it will be shown that if two random composite integers instead of two primes are used, the probability of choosing the integer that divides $\varphi(N)$ reaches 99% if the integers have at least 7 prime factors. Furthermore, the paper suggests an approach to get more information about $\varphi(N)$ without knowing the factorization of N.

The paper is organized as follows. In Section 2, two definitions of the Φ-Hiding assumption are given. Our approach to show that the Φ-Hiding assumption is not valid in certain circumstances is presented in Section 3. Section 4 concludes the paper and outlines areas for future research.

2 The *Φ*-Hiding Assumption

The *Φ*-Hiding assumption [3] can be defined in two different ways. The first definition illustrates the computational problem the assumption is based on.

Definition 1 (*Φ*-Hiding assumption (1)). *Given an integer N with unknown factorization, it is computationally hard to decide whether a prime p_i with $2 < p_i << N^{1/4}$ divides $\varphi(N)$ or not.*[1]

The second definition represents a special case of the assumption, since it is assumed that exactly one of two given integers divides $\varphi(N)$.

Definition 2 (*Φ*-Hiding assumption (2)). *If p_1 and p_2 are two random, small primes and N is constructed such that exactly one of these primes divides $\varphi(N)$, then there is no polynomial-time algorithm to distinguish which of the primes $p_1 > 2$ and $p_2 > 2$ divides $\varphi(N)$ with a probability significantly greater than 0.5, if N is an integer with unknown factorization. If p_i divides $\varphi(N)$, it is said that $\varphi(N)$ hides p_i.*

In cryptographic protocols, Definition 2 of the *Φ*-Hiding assumption is used, since in this case some previous knowledge is involved (i.e. which of the two primes divides $\varphi(N)$), that can be used to create a necessary backdoor for asymmetric cryptography. To the best of our knowledge, no attack on the *Φ*-Hiding assumption has been published until now. In the next Section, we present our approach to show that the *Φ*-Hiding assumption is not valid when Multi-Power RSA moduli are used.

3 The *Φ*-Hiding Assumption Revisited

The *Φ*-Hiding assumption is only valid when it is applied to a composite number that cannot be completely factored in feasible time, since otherwise it would be trivial to decide whether a prime divides $\varphi(N)$ or not. Our approach to decide whether a prime divides $\varphi(N)$ for a composite number N uses the Jacobi symbol. It can be evaluated efficiently, even for composite numbers with unknown factorization [4]. The Jacobi symbol $\mathrm{J}_P(r)$, for P prime, generalizes the Legrende symbol and states information about quadratic residues: If $a^2 \equiv r \pmod{P}$ for given integers r and P has a solution in a, then $\mathrm{J}_P(r) = 1$, otherwise $\mathrm{J}_P(r) = -1$ (if $\gcd(P, r) > 1$, then $\mathrm{J}_P(r) = 0$). For composite odd integers, the Jacobi symbol is defined as $\mathrm{J}_N(r) = \prod_{j=1}^{m} \mathrm{J}_{P_j}(r)^{\nu_j}$, if $N = P_1^{\nu_1} \ldots P_m^{\nu_m}$. Furthermore, a particular $2k$-th root of unity is used to show that the values of the Jacobi symbol are related to

[1] Following the remarks of the original paper of Cachin, Micali and Stadler [3], N can be efficiently factored when a prime $> N^{1/4}$ of $\varphi(N)$ is known, thus the *Φ*-Hiding assumption asks for very small primes. Even if it is known which small primes p_i divide $\varphi(N)$, if $\mathit{log}\ p_i$ is significantly smaller than $(\mathit{log}\ N)^c$, for a constant c between 0 and 1, N cannot be factored significantly faster.

factors of $\varphi(N)$, and that the Jacobi symbol adopts *non-random* values when the evaluated integer r is a divisor of $\varphi(N)$. Thus, the novel idea to use the existence and the non-existence of $2k$-th roots of unity in finite fields/rings allows us to gain knowledge about the divisors of $\varphi(N)$, which in some cases can be used to make the decision whether a given integer divides $\varphi(N)$ or not. These results will be used to show that the Φ-Hiding assumption as defined by Cachin, Micali and Stadler [3] is not valid when applied to a modulus $N = PQ^{2e}$, where $P, Q > 2$ are primes, $e > 0$ is an integer and P hides the prime in question. Lemma 1 is central for our approach:

Lemma 1. *Let ξ_{2k} be any fixed primitive $2k$-th root of unity and $k \in \mathbb{N}^+$, then:*

$$i^{1-k} \prod_{j=1}^{k-1} \left(\xi_{2k}^{j} - \xi_{2k}^{-j} \right) = k \tag{1}$$

Proof (of Lemma 1). The polynomial $f(X) = (X^k - 1)/(X - 1) = X^{k-1} + X^{k-2} + ... + 1$ has ξ_k^j for $j = 1, ..., k-1$ as its roots, where ξ_k is any fixed primitive kth root of unity. Writing $f(X)$ in factored form $f(X) = \prod_{j=1}^{k-1}(X - \xi_k^j)$, we obtain $f(1) = \prod_{j=1}^{k-1}(1 - \xi_k^j) = k$. Since

$$i^{1-k} \prod_{j=1}^{k-1} (\xi_{2k}^{j} - \xi_{2k}^{-j}) = i^{1-k} \prod_{j=1}^{k-1} \xi_{2k}^{j} \prod_{j=1}^{k-1} (1 - \xi_{k}^{-j}) = i^{1-k} k \prod_{j=1}^{k-1} \xi_{2k}^{j} \tag{2}$$

and since $\prod_{j=1}^{k-1} \xi_{2k}^{j} = \xi_{2k}^{(k-1)k/2} = \xi_4^{k-1} = i^{k-1}$, the product $i^{1-k} \prod_{j=1}^{k-1} \xi_{2k}^{j}$ vanishes and we get

$$i^{1-k} \prod_{j=1}^{k-1} (\xi_{2k}^{j} - \xi_{2k}^{-j}) = k \tag{3}$$

which proves the lemma. □

We now rewrite the $(k-1)$ terms covered by the product symbol in equation (1), such that it contains a large square:

Lemma 2 (Square Lemma). *Let $k \in \mathbb{Z}^+$ and $k > 2$. Then:*
1. If k is odd:

$$\prod_{j=1}^{k-1} \left(\xi_{2k}^{j} - \xi_{2k}^{-j} \right) = \prod_{j=1}^{(k-1)/2} \left(\xi_{2k}^{j} + \xi_{2k}^{k-j} \right)^2 \tag{4}$$

2. If k is even:

$$\prod_{j=1}^{k-1} \left(\xi_{2k}^{j} - \xi_{2k}^{-j} \right) = 2i \prod_{j=1}^{(k-2)/2} \left(\xi_{2k}^{j} + \xi_{2k}^{k-j} \right)^2 \tag{5}$$

Proof (of Lemma 2).
1. k is odd: Since k is odd, the jth and the $(k-j)$th factor for $1 \leq j \leq k-1$ can be paired. The result is:

$$\begin{aligned}
&(\xi_{2k}^{j} - \xi_{2k}^{-j}) \cdot (\xi_{2k}^{k-j} - \xi_{2k}^{-(k-j)}) = (\xi_{2k}^{j} - \xi_{2k}^{-j}) \cdot (\xi_{2k}^{k-j} + \xi_{2k}^{j}) \\
&= \xi_{2k}^{j}\xi_{2k}^{k-j} + \xi_{2k}^{j}\xi_{2k}^{j} - \xi_{2k}^{-j}\xi_{2k}^{k-j} - \xi_{2k}^{-j}\xi_{2k}^{j} = -1 + \xi_{2k}^{2j} - \xi_{2k}^{k-2j} - 1 \\
&= \xi_{2k}^{2j} - 2 - \xi_{2k}^{k-2j} = \xi_{2k}^{2j} - 2 + \xi_{2k}^{k}\xi_{2k}^{k-2j} \\
&= \xi_{2k}^{2j} - 2 + \xi_{2k}^{2(k-j)} = (\xi_{2k}^{j} + \xi_{2k}^{k-j})^2
\end{aligned}$$

The pairing contains a square. Since $k-1$ is even, no term is left and a product of $(k-1)/2$ squares is generated, which proves the case for odd values of k.
2. k is even: Since k is even, the jth and the $(k-j)$th factor for $1 \leq j < k/2$ and $k/2 < j \leq k-1$ can be paired, which leads to the same terms as in case 1. The difference is that the factor $\left(\xi_{2k}^{j} - \xi_{2k}^{-j}\right)$ with $j = k/2$ remains. For this factor, $\xi_{2k}^{k/2} - \xi_{2k}^{-k/2} = (-1)^{1/2} - (-1)^{-1/2} = i - i^{-1} = i(1 - 1/i^2) = 2i$, which proves the case for even values of k. □

By Lemma 2, the product in equation (1) is transformed to a product with a perfect square and the factor i^{1-k} (k odd) and $2i^{2-k}$ (k even), respectively.

3.1 Application to Finite Fields and Rings

In this Section, the results are applied to finite fields $\mathbb{F}_P$ with P being a prime number. We distinguish between two cases. In the first case, we assume that a $\xi_{2k} \in \mathbb{F}_P$ does not exist, and in the second case, we assume that a $\xi_{2k} \in \mathbb{F}_P$ exists.

Case 1: A $\xi_{2k} \in \mathbb{F}_P$ does not exist. In this case, it is assumed that $\mathbb{F}_P$ does not contain a $2k$-th root of unity. As a consequence, there is no integer of order $2k$ and thus the factors $\left(\xi_{2k}^{j} + \xi_{2k}^{k-j}\right)$ are not defined properly in $\mathbb{F}_P$. Thus, it cannot be assumed that the product $\prod_{j=1}^{(k-1)/2} \left(\xi_{2k}^{j} + \xi_{2k}^{k-j}\right)^2$ forms a valid square in $\mathbb{F}_P$ and vanishes from the Jacobi symbol. The integer k, which nevertheless exists, has no defined counterpart on the left side of equation 1. In this case, $\mathrm{J}_P(k)$ cannot be distinguished from a random coin flip between 1 and -1.

Case 2: A $\xi_{2k} \in \mathbb{F}_P$ exists. This leads to the fact that the square $\prod_{j=1}^{(k-1)/2} \left(\xi_{2k}^{j} + \xi_{2k}^{k-j}\right)^2$ obtained from Lemma 2 is valid in $\mathbb{F}_P$, since each ξ_{2k} is defined properly. Therefore, equation (1) can be written as a well defined congruence in $\mathbb{F}_P$. Corollary 1 shows the outcome when the Jacobi symbol is applied to this congruence and the square obtained from Lemma 2 is inserted.

Corollary 1. *Let P be an odd prime number, $k \in \mathbb{F}_P$. Assume that a $\xi_{2k} \in \mathbb{F}_P$ exists, then:*
1. If k is odd:

$$\mathrm{J}_P\left((-1)^{(1-k)/2}\prod_{j=1}^{(k-1)/2}\left(\xi_{2k}^{j}+\xi_{2k}^{k-j}\right)^2\right) = J_P((-1)^{(1-k)/2}) = J_P(k) \tag{6}$$

2. If k is even:

$$\mathrm{J}_P\left(2(-1)^{1-k/2}\prod_{j=1}^{(k-2)/2}\left(\xi_{2k}^{j}+\xi_{2k}^{k-j}\right)^2\right) = J_P(2(-1)^{1-k/2}) = J_P(k) \tag{7}$$

After the square has vanished from the Jacobi symbol, a simple congruence is left. This congruence indicates a relationship between the value of the Jacobi symbol and the divisors of $\varphi(P)$, because Corollary 1 is only valid if $2k$ divides $\varphi(P)$. Again, this implicitly shows that it is important to distinguish between the two cases of divisibility introduced above, since the square vanishes only if it is defined properly. Otherwise, the Jacobi symbol of an arbitrary integer k would always be equal to $\mathrm{J}_P((-1)^{(1-k)/2})$ or $\mathrm{J}_P(2(-1)^{1-k/2})$, respectively, which obviously is wrong.

Example: Let $P = 31$ with $\varphi(31) = 30$. By setting $k = 5$ due to $(2 \cdot 5)|30$, there must be an integer of order 10, e.g. 23 or 15. It does not matter which of them is chosen here, since it disappears after applying the Jacobi symbol. Now, calculate $(-1)^{(1-5)/2} = (-1)^{-2} = 1$. Since k is odd, $\mathrm{J}_{31}((-1)^{(1-5)/2}) = \mathrm{J}_{31}(1) = \mathrm{J}_{31}(5)$ must hold, which is true since both sides are equal to 1.

Next, a Theorem is stated that describes the relationship between $\mathrm{J}_P(k)$ and ξ_{2k}.

Theorem 1. *Let P be an odd prime number, $k \in \mathbb{F}_P$. $\mathrm{J}_P(k)$ and the divisors of $\varphi(P)$ are connected via following implications:*
1. If k is odd, then:

$$\begin{aligned} \textit{If } \xi_{2k} \in \mathbb{F}_P \textit{ exists} \quad &\Rightarrow \quad \mathrm{J}_P((-1)^{(1-k)/2}) = \mathrm{J}_P(k). \\ \textit{If } \mathrm{J}_P((-1)^{(1-k)/2}) \neq \mathrm{J}_P(k) \quad &\Rightarrow \quad \xi_{2k} \in \mathbb{F}_P \textit{ does not exist.} \end{aligned}$$

2. If k is even, then:

$$\begin{aligned} \textit{If } \xi_{2k} \in \mathbb{F}_P \textit{ exists} \quad &\Rightarrow \quad \mathrm{J}\left(2(-1)^{1-k/2}\right) = \mathrm{J}_P(k). \\ \textit{If } \mathrm{J}\left(2(-1)^{1-k/2}\right) \neq \mathrm{J}_P(k) \quad &\Rightarrow \quad \xi_{2k} \in \mathbb{F}_P \textit{ does not exist.} \end{aligned}$$

Proof (of theorem 1).
The proof of the Theorem follows directly from Corollary 1. □

Theorem 1 indicates that either a divisor k of $\varphi(P)$ must be known to conclude that the corresponding Jacobi symbols $\mathrm{J}_P(k)$ and $\mathrm{J}_P((-1)^{(1-k)/2})$ (or $\mathrm{J}\left(2(-1)^{1-k/2}\right)$) are equal, or it must be tested whether the two Jacobi symbols $\mathrm{J}_P(k)$ and $\mathrm{J}_P((-1)^{(1-k)/2})$ (or $\mathrm{J}\left(2(-1)^{1-k/2}\right)$) are different in order to get the information that k cannot be a divisor of $\varphi(P)$. In the two other cases, no information can be obtained. The reason is that either the kth root of -1 is not defined, or from the equality of the Jacobi symbols it cannot be concluded that k divides $\varphi(P)$.

To summarize, if $2k$ divides $\varphi(P)$, the Jacobi symbol of k adopts non-random values. Furthermore, Corollary 1 shows that the resulting congruences $\mathrm{J}_P((-1)^{(1-k)/2}) \equiv \mathrm{J}_P(k)$ and $\mathrm{J}_P(2(-1)^{1-k/2}) \equiv \mathrm{J}_P(k)$ for odd and even values of k are *independent* of the chosen ξ_{2k}. Thus, it is only essential that a ξ_{2k} exists in $\mathbb{F}_P$, but it is not necessary to know them.

3.2 Leakage Corollaries

In this Section, we present tables for special composite integers N that contain the values the Jacobi symbol must adopt to leak information about the divisors of $\varphi(N)$. For composite integers N with unknown factorization, we do not know the order of an arbitrary integer a, but we can compute the Jacobi symbol $\mathrm{J}_N(a)$. Thus, we are only able to use the first implication of item 1 and and the second implication of item 2 of Theorem 1. For clarity, the following Corollary divides these items further with respect to different residue classes of a prime P and an integer k.

Corollary 2 (Leakage Corollary for prime numbers). *Let P be an odd prime number, $k \in \mathbb{F}_P$. In any of the following six cases, there does not exist a $\xi_{2k} \in \mathbb{F}_P$.*
If $P \equiv 1 \pmod 4$:

If k is odd: If $\mathrm{J}_P\left(i^{1-k}\right) = 1 \neq -1 = \mathrm{J}_P(k)$.
If k is even: If $\mathrm{J}_P\left(2i^{2-k}\right) = (-1)^{(p^2-1)/8} \neq \mathrm{J}_P(k)$.

If $P \equiv 3 \pmod 4$:

If $k \equiv 0 \pmod 4$: If $\mathrm{J}_P\left(2(-1)^{1-k/2}\right) = (-1)^{(P^2+7)/8} \neq \mathrm{J}_P(k)$.
If $k \equiv 1 \pmod 4$: If $\mathrm{J}_P\left((-1)^{(1-k)/2}\right) = 1 \neq \mathrm{J}_P(k)$.
If $k \equiv 2 \pmod 4$: If $\mathrm{J}_P\left(2(-1)^{1-k/2}\right) = (-1)^{(P^2-1)/8} \neq \mathrm{J}_P(k)$.
If $k \equiv 3 \pmod 4$: If $\mathrm{J}_P\left((-1)^{(1-k)/2}\right) = -1 \neq \mathrm{J}_P(k)$.

The Corollary states which two Jacobi symbols must differ to be sure that the integer k is not a divisor of $\varphi(P)$. Thus, in some cases, the access to the Jacobi symbol is sufficient to decide whether a prime divides $P-1$ or not. Next, the Corollary is extended to composite integers N being the product of two distinct prime numbers P and Q. This leads to the tables shown in figure 1. The tables must be read in the following way: The four tables handle the four different residues of k modulo 4. Furthermore, the first two tables (horizontal direction) show the 64 combinations of the 8 different residues of P and Q modulo 16 ($P, Q > 2$) for even residues of k. The third tables

Q \ P								
k=0+4s	1	3	5	7	9	11	13	15
1	-1	-1	+1	+1	-1	-1	+1	+1
3	-1	-1	+1	+1	-1	-1	+1	+1
5	+1	+1	-1	-1	+1	+1	-1	-1
7	+1	+1	-1	-1	+1	+1	-1	-1
9	-1	-1	+1	+1	-1	-1	+1	+1
11	-1	-1	+1	+1	-1	-1	+1	+1
13	+1	+1	-1	-1	+1	+1	-1	-1
15	+1	+1	-1	-1	+1	+1	-1	-1

Q \ P								
k=2+4s	1	3	5	7	9	11	13	15
1	-1	+1	+1	-1	-1	+1	+1	-1
3	+1	-1	-1	+1	+1	-1	-1	+1
5	+1	-1	-1	+1	+1	-1	-1	+1
7	-1	+1	+1	-1	-1	+1	+1	-1
9	-1	+1	+1	-1	-1	+1	+1	-1
11	+1	-1	-1	+1	+1	-1	-1	+1
13	+1	-1	-1	+1	+1	-1	-1	+1
15	-1	+1	+1	-1	-1	+1	+1	-1

Q \ P								
k=1+4s	1	3	5	7	9	11	13	15
*	-1	-1	-1	-1	-1	-1	-1	-1

Q \ P								
k=3+4s	1	3	5	7	9	11	13	15
1	-1	+1	+1	-1	-1	+1	+1	-1
3	+1	-1	+1	-1	+1	-1	+1	-1
5	-1	+1	+1	-1	-1	+1	+1	-1
7	+1	-1	+1	-1	+1	-1	+1	-1
9	-1	+1	+1	-1	-1	+1	+1	-1
11	+1	-1	+1	-1	+1	-1	+1	-1
13	-1	+1	+1	-1	-1	+1	+1	-1
15	+1	-1	+1	-1	+1	-1	+1	-1

Fig. 1. Entries: $\mathrm{J}_{PQ}(k)$. Tables for $N = PQ$ for different residues of P and Q modulo 16.

was reduced to one a single row since it contains 64 values of -1. The fourth table shows the 64 combinations of the 8 different residues of P and Q modulo 16 ($P, Q > 2$) for $k \equiv 3 \pmod 4$. The entries for each combination of P and Q illustrate which value of the Jacobi symbol $\mathrm{J}_N(k)$ reveals that there is no integer of order $2k$ for at least one of the primes P and Q. For example, the first entry of -1 in the upper left table represents the case $k \equiv 0 \pmod 4$ and $P \equiv Q \equiv 1 \pmod{16}$. Applying Corollary 2 to this combination yields $\mathrm{J}_P\left(2i^{2-k}\right) = \mathrm{J}_Q\left(2i^{2-k}\right) = 1$. The corresponding table entry of -1 shows that $\mathrm{J}_N(k)$ must be -1, therefore at least for one of the primes P or Q, there is no integer of order $2k$.

The conclusion is too weak to obtain knowledge regarding the Φ-Hiding assumption, since $\phi(N)$ could still be divisible by $2k$. Some integers, even with unknown factorization, allow to obtain more information about the divisors of $\varphi(N)$. These are integers of the form $N = PQ^{2e}$, since one of the two involved primes is a square, which is ignored by the Jacobi symbol. In this way, the Jacobi symbol leaks information about the other prime involved. If N has the form $N = PQ^{2e}$, then for the Jacobi symbol and a co-prime integer $k > 2$, $\mathrm{J}_N(k) = \mathrm{J}_{PQ^{2e}}(k) = \mathrm{J}_P(k) \cdot \mathrm{J}_Q(k)^{2e} = \mathrm{J}_P(k)$.

Using this fact, the tables displayed in figure 2 show the values the Jacobi symbol $\mathrm{J}_N(k)$ must adopt such that $2k$ does not divide $\varphi(P)$.

Example: Suppose $N = 1323801442080750176044871$ and N is of the form $N = PQ^{2e}$, $e > 0$. Suppose we want to test whether $k = 41$ divides $P - 1$. Since $k \equiv 1 \pmod 4$, the third table must be used. Thus, $\mathrm{J}_N(41) = -1$. The table shows that whenever the Jacobi symbol of k is negative, k can not divide $P - 1$.

Q \ P								
k=0+4s	1	3	5	7	9	11	13	15
*	-1	-1	+1	+1	-1	-1	+1	+1

Q \ P								
k=2+4s	1	3	5	7	9	11	13	15
*	-1	+1	+1	-1	-1	+1	+1	-1

Q \ P								
k=1+4s	1	3	5	7	9	11	13	15
*	-1	-1	-1	-1	-1	-1	-1	-1

Q \ P								
k=3+4s	1	3	5	7	9	11	13	15
*	-1	+1	-1	+1	-1	+1	-1	+1

Fig. 2. Entries: $\mathrm{J}_{PQ^{2e}}(k)$. Tables for $N = PQ^{2e}$ for different residues of P and Q modulo 16.

In the next Section, the last two tables are used to invalidate the Φ-Hiding assumption when using moduli of the form $N = PQ^{2e}$ and choosing P to hide the prime number in question.

3.3 Application to the Φ-Hiding Assumption

In both Definitions 1 and 2 of Section 2, it is only required that N is a composite integer with unknown factorization. By applying our results from the previous Sections, we show that this requirement is not sufficient. If the Φ-Hiding assumption is applied to a modulus of the form PQ^{2e}, where the integer P is constructed in such a way that P hides a given prime, then the Φ-Hiding assumption is violated with non-negligible probability. Moduli of this form, mostly with $e = 1$, are used by several cryptographic protocols, as described by Boneh and Shacham [1] and used, e.g., by Poupard and Stern [8], to speed up some computations that profit from the form PQ^{2e} with $e > 0$ instead of PQ. Using the results of the previous Sections, the following Theorem can be stated:

Theorem 2. *Let $N = PQ^{2e}$ and suppose that P hides p. Then, the Φ-Hiding assumption from Definition 2 can be violated. An attacker can choose the hidden prime with an average success probability of $\frac{3}{4}$.*

The following notation is used: N is again of the form $N = PQ^2$ and $\mathrm{T}(N, k)$ is the value of the corresponding table entry of figure 2.

Proof (of Theorem 2). Suppose that either p_1 or p_2 divides $\varphi(N)$ and an attacker has to decide which of them divides $\varphi(N)$. Without loss of generality, we assume that p_1 is the prime that is hidden by P. For this prime, $\mathrm{J}_N(p_1) \neq \mathrm{T}(N, p_1)$ holds, because it divides $P - 1$ (see Theorem 1).

Thus, the attacker will find *at least* one matching Jacobi symbol concerning the primes p_1 and p_2. From the attackers point of view, the probability that a prime p_i, $i \in \{1, 2\}$ divides $\varphi(N)$ is

$$Prob[p_i|\varphi(N)] = \begin{cases} 0, & \mathrm{J}_N(p_i) = \mathrm{T}(N, p_i) \\ 1, & \mathrm{J}_N(\overline{p}_i) = \mathrm{T}(N, \overline{p}_i) \\ \frac{1}{2}, & \mathrm{J}_N(p_i) = \mathrm{J}_N(\overline{p}_i) \end{cases} \tag{8}$$

where $\overline{p}_i$ denotes the other one of the two primes. Note the factorization of N is not needed to construct the tables in figure 2. They are universally valid for moduli of the form $N = PQ^{2e}$ and thus known to the attacker. Whenever the Jacobi symbol $\mathrm{J}_N(p_i)$ is equal to $\mathrm{T}(N, p_i)$, Theorem 1 states that p_i cannot be a divisor of $\varphi(N)$, thus the probability is $Prob[p_i|\varphi(N)] = 0$. Consequently, the Jacobi symbol $\mathrm{J}_N(\overline{p}_i)$ must be not equal to $T(N, \overline{p}_i)$, which indicates that it is the hidden prime. If both Jacobi symbols do not match the table entry, no information is leaked and the attacker cannot argue in any direction. Thus, in this case the probability is $Prob[p_i|\varphi(N)] = \frac{1}{2}$. Since the primes p_i are chosen randomly, it can be assumed that the Jacobi symbol $\mathrm{J}_N(p_2)$ adopts random values of -1 and $+1$. The calculation of the total probability for the attacker to choose the hidden prime correctly is as follows: Whenever a Jacobi symbol evaluates to a value unequal to the table entry, it cannot be the prime that is hidden by P, so the attacker chooses the other one, the hidden one, with a probability of 1. When both Jacobi symbols evaluate to $\neq \mathrm{T}(N, \cdot)$, the attacker chooses the right one with a probability of $\frac{1}{2}$. Thus, in total there is an average probability of $\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$ to choose the correct prime, which proves Theorem 2. □

Composite Integers. The situation is even worse when the *Φ*-Hiding assumption is used with composite integers n_1 and n_2 instead of the primes p_1 and p_2, as done, for example, by Gentry et al. [5]. Assume that there is a modulus of the form $N = PQ^2$ and we want to determine whether the composite integer n_i, which is the product of m distinct primes greater than 2, divides $\varphi(N)$. Suppose the Jacobi symbol is applied and the result does not allow to decide whether n_i divides $\varphi(N)$ or not. In this case, we can proceed with the prime factors of n_i. Since n_i is $\prod_{j=1}^{m} p_j$, the Jacobi symbol can simply be evaluated for all of its prime factors. If there is a prime p_j with a Jacobi symbol that leaks the required information, we know that n_i cannot divide $\varphi(N)$, since from $n_i|\varphi(N)$ it follows that $p_j|\varphi(N)$ must also hold. If the integers in question consist only of 7 prime numbers, there already is a success probability of $\approx 99\%$ to choose the right integer.

Corollary 3. *If* $n_1 = \prod_{j=1}^{l_1} p_i$ *and* $n_2 = \prod_{j=1}^{l_2} q_j$ *are two random, composite integers that are odd and square free and* n_1 *is the hidden integer, then an attacker has a success probability of* $(1 - \frac{1}{2^{l_2}})$ *to choose the hidden integer.*

Proof. Let $n_1 = \prod_{j=1}^{l_1} p_j$ and $n_2 = \prod_{j=1}^{l_2} q_j$ be two odd, square free integers. If $N = PQ^{2e}$ and exactly one of the two integers n_1 and n_2 divides $\varphi(N)$, the probability to choose the right one of

the two possibilities is as follows. The case $l_1 = l_2 = 1$ was already addressed in the paper; it has a success probability of $\frac{3}{4}$. Note that if $n_i | \varphi(N)$, then also each divisor of n_i is a divisor of N. Thus, if we find a divisor of n_i that does not divide $\varphi(N)$, we can conclude that n_i is not the integer hidden by $\varphi(N)$. Since the same argument applies to all divisors that are prime numbers, it is sufficient to check all prime factors of n_i whether they are divisors of $\varphi(N)$ or not.
Without loss of generality, we assume that n_1 is the integer hidden by $\varphi(N)$. For each of its l_1 prime factors p_i, $\mathrm{J}_N(p_i) \neq \mathrm{T}(N, p_i)$ must hold. For the other integer n_2, it follows that for each of its l_2 prime factors q_i it holds with a probability of $\frac{1}{2}$ that $\mathrm{J}_N(q_i) \neq \mathrm{T}(N, q_i)$ and with a probability of $\frac{1}{2}$ that $\mathrm{J}_N(q_i) = \mathrm{T}(N, q_i)$. Whenever the first case occurs, no knowledge is gained. But whenever the latter case occurs, the information that n_2 cannot be a divisor of $\varphi(N)$ is gained, so n_1 is the hidden number. The method fails if for all prime factors $\mathrm{J}_N(q_i) \neq \mathrm{T}(N, q_i)$ is obtained, which occurs with a probability of $\prod_{i=1}^{l_2} Prob[\mathrm{J}_N(q_i) \neq \mathrm{T}(N, q_i)] = \frac{1}{2^{l_2}}$. Thus, the success probability of choosing the right integer is $(1 - \frac{1}{2^{l_2}})$. □

Table 1 illustrates the success probability of choosing the right prime for different numbers of prime factors.

$l_1 = l_2$	1	2	3	4	5	6	7
	0.5	0.75	0.875	0.938	0.969	0.984	0.992

Table 1. Success Probability

3.4 Discussion

In the previous Section we have shown that in some circumstances it can be efficiently decided whether a given prime p divides $\varphi(N)$ or not. A necessary condition is that moduli of the form PQ^{2e} with $e > 1$ are used and P hides p. If someone implements a cryptographic protocol based on the Φ-Hiding assumption and uses such moduli, an attacker has an average probability of $\frac{3}{4}$ to choose the right prime, if the primes the attacker can choose from are selected randomly. In cases when it is desired to ask which composite number n_i is hidden by P, the success probability would be even greater than $\frac{3}{4}$, since for each prime factor of n the attacker has the success probability of $\frac{3}{4}$. There are two possible countermeasures to the presented attack. First, moduli of the form $PQ^{2e}, e > 1$ should not be used in conjunction with the Φ-Hiding assumption. Second, the primes a user can choose from should not be selected randomly, but only those primes that have a positive Jacobi symbol regarding N should be used. Thus, the assumption as stated in the original form should be adapted to avoid its vulnerability to the presented attack.

4 Conclusions

In this paper, it was shown that by utilizing an identity of $2k$-th roots in $\mathbb{Z}_N$ and the Jacobi symbol, it is possible to gain knowledge about the unknown factors of Euler's totient function $\varphi(N)$ even if N is computationally hard to factorize. This knowledge was used to invalidate the Φ-Hiding assumption as defined by Cachin, Micali and Stadler [3] for moduli of the form $N = PQ^{2e}$ with P hiding the prime in question, since the Jacobi symbol adopts non-random values when being applied to a factor of $\varphi(N)$. Our results are important for evaluating the security of cryptographic protocols that use the Φ-Hiding assumption and exemplify the situation when it has to handled with care. There are several areas for future work. For example, an interesting issue is to examine the case when the integer k does not divide $\varphi(N)$. In this case, the identity is not well defined. Thus, it should be investigated whether there are methods to bypass this problem to obtain further relationships between the Jacobi symbol and the factors of $\varphi(N)$. Since the approach makes use of an identity of $2k$-th roots in $\mathbb{Z}_N$ and this identity is only one of many, future work should be directed to analyze other results of such identities that may offer attack possibilities on the Φ-Hiding assumption.

Acknowledgements. The authors would like to thank Frederik Vercauteren for his excellent comments to improve the presentation of the material in this paper.

References

1. Dan Boneh and Hovav Shacham. Fast Variants of RSA. *CryptoBytes*, 5(1), Winter/Spring 2002.
2. Christian Cachin. Efficient Private Bidding and Auctions with an Oblivious Third Party. In *ACM Conference on Computer and Communications Security*, pages 120–127, 1999.
3. Christian Cachin, Silvio Micali, and Markus Stadler. Computationally Private Information Retrieval with Polylogarithmic Communication. *Advances in Cryptology - EUROCRYPT '99*, 1592:402–407, 1999.
4. Shawna Meyer Eikenberry and Jonathan P. Sorenson. Efficient Algorithms for Computing the Jacobi Symbol. *Journal of Symbolic Computation*, 26(4):509–523, 1998.
5. Craig Gentry, Philip Mackenzie, and Zulfikar Ramzan. Password Authenticated Key Exchange Using Hidden Smooth Subgroups. In *Proceedings of the 12th ACM Conference on Computer and Communications Security*, pages 299–309, New York, NY, USA, 2005. ACM Press.
6. Craig Gentry and Zulfikar Ramzan. Single-Database Private Information Retrieval with Constant Communication Rate. In *Proceedings of the 32nd International Colloquium on Automata, Languages and Programming, Lisbon, Portugal*, pages 803–815, 2005.
7. Brett Hemenway and Rafail Ostrovsky. Public Key Encryption which is Simultaneously a Locally-Decodable Error-Correcting Code. In *Electronic Colloquium on Computational Complexity, Report No. 21*, 2007.
8. Guillaume Poupard and Jacques Stern. Fair Encryption of RSA Keys. In *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT)*, pages 172–189, 2000.