3. Desmedt–Odlyzko's Attack

Desmedt and Odlyzko's attack is an existential forgery under a chosen-message attack, in which the forger asks for the signature of messages of his choice before computing the signature of a (possibly meaningless) message that was never signed by the legitimate owner of d. In the case of Rabin–Williams signatures, it may even happen that the attacker factors N, i.e., a total break. The attack only applies if $\mu(m)$ is much smaller than N and works as follows:

1. Select a bound B and let $\mathfrak{P} = \{p_1, \ldots, p_\ell\}$ be the list of all primes less or equal to B.
2. Find at least $\tau \geq \ell + 1$ messages m_i such that each $\mu(m_i)$ is a product of primes in $\mathfrak{P}$.
3. Express one $\mu(m_j)$ as a multiplicative combination of the other $\mu(m_i)$, by solving a linear system given by the exponent vectors of the $\mu(m_i)$ with respect to the primes in $\mathfrak{P}$.
4. Ask for the signatures of the m_i for $i \neq j$ and forge the signature of m_j.

In the following, we assume that e is prime; this includes $e = 2$. We let τ be the number of messages m_i obtained at step 2. We say that an integer is B-smooth if all its prime factors are less or equal to B. The integers $\mu(m_i)$ obtained at step 2 are therefore B-smooth, and we can write for all messages m_i, $1 \leq i \leq \tau$:

$$\mu(m_i) = \prod_{j=1}^{\ell} p_j^{v_{i,j}} \tag{1}$$

To each $\mu(m_i)$, we associate the ℓ-dimensional vector of the exponents modulo e, that is, $\boldsymbol{V_i} = (v_{i,1} \bmod e, \ldots, v_{i,\ell} \bmod e)$. Since e is prime, the set of all ℓ-dimensional vectors modulo e forms a linear space of dimension ℓ. Therefore, if $\tau \geq \ell + 1$, one can express one vector, say $\boldsymbol{V_\tau}$, as a linear combination of the others modulo e, using Gaussian elimination:

$$\boldsymbol{V_\tau} = \boldsymbol{\Gamma} \cdot e + \sum_{i=1}^{\tau-1} \beta_i \boldsymbol{V_i}$$

for some $\boldsymbol{\Gamma} = (\gamma_1, \dots, \gamma_\ell) \in \mathbb{Z}^\ell$ and some $\beta_i \in \{0, \dots, e-1\}$. This gives for all $1 \le j \le \ell$:

$$v_{\tau,j} = \gamma_j \cdot e + \sum_{i=1}^{\tau-1} \beta_i \cdot v_{i,j}$$

Then using (1), one obtains:

$$\mu(m_\tau) = \prod_{j=1}^{\ell} p_j^{v_{\tau,j}} = \prod_{j=1}^{\ell} p_j^{\gamma_j \cdot e + \sum_{i=1}^{\tau-1} \beta_i \cdot v_{i,j}} = \left(\prod_{j=1}^{\ell} p_j^{\gamma_j} \right)^e \cdot \prod_{j=1}^{\ell} \prod_{i=1}^{\tau-1} p_j^{v_{i,j} \cdot \beta_i}$$

$$\mu(m_\tau) = \left(\prod_{j=1}^{\ell} p_j^{\gamma_j} \right)^e \cdot \prod_{i=1}^{\tau-1} \left(\prod_{j=1}^{\ell} p_j^{v_{i,j}} \right)^{\beta_i} = \left(\prod_{j=1}^{\ell} p_j^{\gamma_j} \right)^e \cdot \prod_{i=1}^{\tau-1} \mu(m_i)^{\beta_i}$$

That is:

$$\mu(m_\tau) = \delta^e \cdot \prod_{i=1}^{\tau-1} \mu(m_i)^{\beta_i}, \text{ where } \delta := \prod_{j=1}^{\ell} p_j^{\gamma_j} \tag{2}$$

Therefore, we see that $\mu(m_\tau)$ can be written as a multiplicative combination of the other $\mu(m_i)$. For RSA signatures, the attacker will ask for the signatures σ_i of $m_1, \dots, m_{\tau-1}$ and forge the signature σ_τ of m_τ using the relation:

$$\sigma_\tau = \mu(m_\tau)^d = \delta \cdot \prod_{i=1}^{\tau-1} \left(\mu(m_i)^d \right)^{\beta_i} = \delta \cdot \prod_{i=1}^{\tau-1} \sigma_i^{\beta_i} \pmod N$$

3.1. *Rabin–Williams Signatures*

For Rabin–Williams signatures ($e = 2$), the attacker may even factor N. Let $\mathrm{J}(x)$ denote the Jacobi symbol of x with respect to N. We distinguish two cases. If $\mathrm{J}(\delta) = 1$, we have $\delta^{2d} = \pm\delta \bmod N$, which gives from (2) the forgery equation:

$$\mu(m_\tau)^d = \pm\delta \cdot \prod_{i=1}^{\tau-1} \left(\mu(m_i)^d \right)^{\beta_i} \pmod N$$

If $\mathrm{J}(\delta) = -1$, then letting $u = \delta^{2d} \bmod N$ we obtain $u^2 = (\delta^2)^{2d} = \delta^2 \bmod N$, which implies $(u - \delta)(u + \delta) = 0 \bmod N$. Moreover since $\mathrm{J}(\delta) = -\mathrm{J}(u)$, we must have $\delta \neq \pm u \bmod N$, and therefore, $\gcd(u \pm \delta, N)$ will factor N. The attacker can therefore

Table 1. The value of Dickman's function for $1 \leq t \leq 10$.

t	1	2	3	4	5	6	7	8	9	10
$-\log_2 \rho(t)$	0.0	1.7	4.4	7.7	11.5	15.6	20.1	24.9	29.9	35.1

submit the τ messages for signature, recover $u = \delta^{2d} \bmod N$, factor N and subsequently sign any message.[2]

3.2. *Attack Complexity*

The complexity of the attack depends on the number of primes ℓ and on the probability that the integers $\mu(m_i)$ are p_ℓ-smooth, where p_ℓ is the ℓth prime. We define $\psi(x, y) = \#\{v \leq x$, such thatv is y− smooth$\}$. It is known [22] that, for large x, the ratio $\psi(x, \sqrt[t]{x})/x$ is equivalent to Dickman's function defined by:

$$\rho(t) = \begin{cases} 1 & \text{if } 0 \leq t \leq 1 \\ \rho(n) - \displaystyle\int_n^t \frac{\rho(v-1)}{v} dv & \text{if } n \leq t \leq n+1 \end{cases}$$

$\rho(t)$ is thus an approximation of the probability that a u-bit number is $2^{u/t}$-smooth; Table 1 gives the numerical value of $\rho(t)$ (on a logarithmic scale) for $1 \leq t \leq 10$. The following theorem [12] gives an asymptotic estimate of the probability that an integer is smooth:

Theorem 1. *Let x be an integer and let $L_x[\beta] = \exp\left(\beta \cdot \sqrt{\log x \log\log x}\right)$. Let t be an integer randomly distributed between zero and x^γ for some $\gamma > 0$. Then for large x, the probability that all the prime factors of t are less than $L_x[\beta]$ is given by $L_x\left[-\gamma/(2\beta) + o(1)\right]$.*

Using this theorem, an asymptotic analysis of Desmedt and Odlyzko's attack is given in [17]. The analysis yields a time complexity of:

$$L_x[\sqrt{2} + o(1)]$$

where x is a bound on $\mu(m)$. This complexity is sub-exponential in the size of the integers $\mu(m)$. In practice, the attack is feasible only if the $\mu(m_i)$ is relatively small (e.g., <200 bits).

[2] In both cases, we have assumed that the signature is always $\sigma = \mu(m)^d \bmod N$, whereas by definition, a Rabin–Williams signature is $\sigma = (\mu(m)/2)^d \bmod N$ when $\mathrm{J}(\mu(m)) = -1$. A possible work-around consists in discarding such messages, but it is also easy to adapt the attack to handle both cases.