Eliding RSA Group Membership Checks

Dr Adam Everspaugh, Michael Lodder

October 2020

Background. Our tEcdsa specification [1] requires that we verify that certain (security-sensitive) randomly-selected numbers are members of an RSA group. That is, select $x \in \mathbb{Z}_N^*$ where $N = pq$ for large primes p, q. The simplest implementation of this, given N with no knowledge of p, q, is to select a random value from the range $(0, N)$ and then test for group membership in $\mathbb{Z}_N^*$. Choosing a value uniformly at random from that interval is performant, but determining $gcd(x, N) \neq 1$ is not, because GCD computation, while still polynomial in time complexity, is not performant.

We would prefer to avoid this membership test to improve the performance of our implementation.

To that end, we prove that when N is a composite value with only 2 (large) prime factors, then a random value from the range $(0, N)$ will be in $\mathbb{Z}_N^*$ with overwhelming probability. Note, this is not surprising. If this were not the case, RSA security would be undermined by the selection of random values (polynomial time) and GCD computation (also polynomial time).

Preliminaries. We denote the additive group on integers that are co-prime to m as $\mathbb{Z}_m^*$. And we use the following asymptotic definition of negligible functions from [2].

Definition 1 (Negligible function)**.** *A function f is* negligible *if for every polynomial $p(\cdot)$ $\exists N$ such that $\forall n > N$: $f(n) < n^{-c}$.*

With this definition, in the asymptotic security model, it is enough to show that the probability that a value x selected uniformly at random from $\mathbb{Z}_N$ is not a member of $\mathbb{Z}_N^*$ is negligible.

Theorem 1. *Let λ be our security parameter, $N = pq$, with p, q primes, and $\log p = \log q = \lambda$. If $x \xleftarrow{\$} \mathbb{Z}_N$, then the probability that $x \notin \mathbb{Z}_N^*$ is negligible in λ.*

Proof. $\mathbb{Z}_N^* = \{x \mid gcd(x, N) = 1\}$ by definition. We note that N has exactly two prime factors, and so the set of of non-members are exactly the set of multiples of p or q: $\{kp, kq \mid k \in \mathbb{Z}\}$.

Let x be a value selected uniformly at random from $\mathbb{Z}_N$, and so the density of non-members to all values in $\mathbb{Z}_N$ is the ratio (excluding constants):

$$\frac{p+q}{pq}.$$

wlog we take p to be the smaller of p,q and so:

$$\frac{p+q}{pq} \leq \frac{q+q}{qq} = \frac{2q}{q^2} = 2q^{-1}.$$

And so the probability of $x \notin \mathbb{Z}_N^*$ is negligible in q, which is itself a function of the security parameter λ. □

Proof by security reduction. As mentioned above, this result is not surprising. We give an alternate, informal proof by security reduction. Selecting a random value can be done in polynomial time, computing $gcd(x, N)$ can also be done in polynomial time via the extended Euclidean algorithm, which also gives a factorization of N as a function of x. If x were not in the group $\mathbb{Z}_N^*$, then $x = kp$ or $x = kq$ and a polynomial-time-bound adversary now holds this factorization in-hand. With this factorization, one can compute p, q and then Euler's totient $\phi(N)$ which is the secret key for RSA. Hence, the security of this method reduces to the security of the RSA cryptosystem.

References

[1] *Threshold ECDSA Pseudocode for Coinbase*, 2020.

[2] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography, Second Edition.* Chapman amp; Hall/CRC, 2nd edition, 2014.