On the Security of Trapdoor Subgroups of $\mathbb{Z}_N^*$

Marc Joye

marc.joye@gmail.com

In a recent work, Park, Lee and Lee [1] present an identity-based encryption scheme and a companion signature scheme. Interestingly, their schemes work in RSA subgroups. The authors introduce two security assumptions to prove the security of their schemes. We show in this short note that, unfortunately, the assumptions do not hold.

Assumptions. Consider PPT algorithm $\mathsf{TRSAgen}$ which, on input a security parameter 1^κ, generates an RSA modulus $N = pq$ where $p = 2p_1+1$ and $q = 2q_1+1$, with p, q, p_1, q_1 prime, an element $g \in \mathbb{Z}_N^*$ of order p_1q_1, and a length ℓ for some $\ell < |p_1q_1|$. We write $(N, g, l) \leftarrow \mathsf{TRSAgen}(1^\kappa)$.

Assumption 1 (TSDH Assumption). *With the previous notations, the $\tilde{q}$-TSDH assumption asserts that*

$$\Pr\left[\mathcal{A}\left(N, g, g^x, g^{(x+r_0)y}, r_0, \left\{\left(1/(x+r_i), r_i\right)\right\}_{i=1}^{\tilde{q}}\right) = g^y\right]$$

is negligible for any PPT algorithm $\mathcal{A}$; the probabilities are taken over the experiment of running $(N, g, \ell) \leftarrow \mathsf{TRSAgen}(1^\kappa)$ and choosing at random $x, y \in \mathbb{Z}_{p_1q_1}$ and $r_0, r_1, \ldots, r_{\tilde{q}} \in \{0,1\}^\ell$.

Assumption 2 (TSEI Assumption). *With the previous notations, the $\tilde{q}$-TSEI assumption asserts that*

$$\Pr\left[\mathcal{A}\left(N, g, g^x, \left\{\left(1/(x+r_i), r_i\right)\right\}_{i=1}^{\tilde{q}}\right) = \left(1/(x+r^*), r^*\right) \mid r^* \notin \{r_1, \ldots, r_{\tilde{q}}\}\right]$$

is negligible for any PPT algorithm $\mathcal{A}$; the probabilities are taken over the experiment of running $(N, g, \ell) \leftarrow \mathsf{TRSAgen}(1^\kappa)$ and choosing at random $x \in \mathbb{Z}_{p_1q_1}$ and $r_1, \ldots, r_{\tilde{q}} \in \{0,1\}^\ell$.

Analysis. Define the set $\mathscr{S} = \left\{(\sigma_i, r_i)\right\}_{i=1}^{\tilde{q}}$ where $\sigma_i = 1/(x+r_i) \pmod{p_1q_1}$. From a pair of elements $(\sigma_1, r_1), (\sigma_2, r_2) \in \mathscr{S}$, it is easily checked that

$$\sigma_1\sigma_2(r_1 - r_2) + \sigma_1 - \sigma_2 \equiv 0 \pmod{p_1q_1} \ .$$

We can write $\Lambda := \sigma_1\sigma_2(r_1 - r_2) + \sigma_1 - \sigma_2$ as $\Lambda = 2^t\Lambda_0$ where $2^t \| \Lambda$ and Λ_0 is odd. It is worth observing that $\Lambda_0 \propto p_1q_1$. Next we choose a random element $h \in \mathbb{Z}_N^*$ with Jacobi symbol -1. It follows then that

$$\gcd(h^{\Lambda_0} \pm 1 \bmod N, N)$$

yields the factorization of N. Indeed, since $\left(\frac{h}{N}\right) = -1$, we can assume without loss of generality that $\left(\frac{h}{p}\right) = 1$ and $\left(\frac{h}{q}\right) = -1$. Hence, letting $\alpha = \Lambda_0/p_1$ and $\beta = \Lambda_0/q_1$ in $\mathbb{Z}$, we have $h^{\Lambda_0} \equiv \left(\frac{h}{p}\right)^\alpha \equiv 1 \pmod{p}$ and $h^{\Lambda_0} \equiv \left(\frac{h}{q}\right)^\beta \equiv -1 \pmod{p}$ since β is odd. In turn, this implies that $\gcd(h^{\Lambda_0} - 1 \bmod N, N) = p$ and $\gcd(h^{\Lambda_0} + 1 \bmod N, N) = q$. Hence, we get $p_1q_1 = (p-1)(q-1)/4$.

Once p_1q_1 is known, an attacker against the TSDH assumption can recover x from (σ_1, r_1) as $x = (1/\sigma_1) - r_1 \bmod p_1q_1$ and next $z := g^y \bmod N$ as $z = (g^{(x+r_0)y})^\gamma \bmod N$ where $\gamma := 1/(x+r_0) \bmod p_1q_1$.

Similarly, an attacker against the TSEI assumption can first recover x from (σ_1, r_1) and then compute a new pair $(1/(x+r^*) \bmod p_1q_1, r^*)$ for any chosen $r^* \in \{0,1\}^\ell$.

Extension. The authors of [1] more generally consider the case of RSA moduli of the form $N = pq$ where $p = 2p_1 \cdots p_I + 1$ and $q = 2q_1 \cdots q_J + 1$ with $p_1, \dots, p_I$ and $q_1, \dots, q_J$ prime, and p_1q_1-order subgroups of $\mathbb{Z}_N^*$. In this case, an attacker, from two pairs (σ_1, r_1) and (σ_2, r_2) where $\sigma_i = 1/(x + r_i) \bmod p_1q_1$ with $i \in \{1, 2\}$, can compute $\mathit{\Lambda}$ as

$$\mathit{\Lambda} := \sigma_1\sigma_2(r_1 - r_2) + \sigma_1 - \sigma_2 \ .$$

Again the main observation is that the so-defined $\mathit{\Lambda}$ is a multiple of p_1q_1.

Given two integers a and b whose prime factorizations are $a = \prod_{i \in \mathscr{I}} {p_i}^{e_i}$ and $b = \prod_{j \in \mathscr{J}} {p_i}^{f_i}$ with $e_i, f_i > 0$, we define the operator $\mathrm{cop}_b(a) = \prod_{i \in \mathscr{I}, i \notin \mathscr{J}} {p_i}^{e_i}$. This can be obtained by successive GCDs:

```
$\delta \leftarrow \gcd(a, b)$
until $(\delta = 1)$ do
    $a \leftarrow a/\delta$; $\delta \leftarrow \gcd(a, b)$
return $a$
```

Against the TSDH assumption, the attacker computes

$$x' := (1/\sigma_1) - r_1 \bmod \mathrm{cop}_{\sigma_1}(\mathit{\Lambda})\,, \quad \gamma := 1/(x' + r_0) \bmod \mathrm{cop}_{(x'+r_0)}(\mathit{\Lambda})$$

and then recovers $z := g^y \bmod N$ as

$$z = \left(g^{(x+r_0)y}\right)^{\gamma} \bmod N \ .$$

For the TSEI assumption, an attacker needs to produce a pair $(1/(x + r^*), r^*)$ where the first component is computed modulo p_1q_1. The knowledge of a multiple of p_1q_1 (i.e., $\mathit{\Lambda}$) is not enough. However, by considering more than two pairs (σ_i, r_i), the attacker can easily obtain p_1q_1; namely

$$\mathit{\Lambda}' := \gcd\bigl(\sigma_1\sigma_2(r_1 - r_2) + \sigma_1 - \sigma_2, \sigma_1\sigma_3(r_1 - r_3) + \sigma_1 - \sigma_3\bigr)$$

is likely to be equal to p_1q_1 or a small multiple thereof (that allows the recovery of p_1q_1 by pulling out its small factors).

References

1. Jong Hwan Park, Kwangsu Lee, and Dong Hoon Lee. Efficient identity-based encryption and public-key signature from trapdoor subgroups. Cryptology ePrint Archive, Report 2016/500, 2016. http://eprint.iacr.org/.