C.P. Schnorr: Security of 2^t–Root Identification and Signatures, Proceedings CRYPTO'96, Springer LNCS 1109, (1996), pp. 143–156
page 148, section 3, line 5 of the proof of Theorem 3.
Correction. The proposed factoring method

$$\text{Check whether } \{\gcd(Y^{2^i} \pm Z^{2^{i+\ell}}, N)\} = \{p, q\} \text{ holds for some } i \text{ with } 0 \le i < t$$

fails if $Y^{2^i} = -Z^{2^{i+\ell}}$ holds for some i with $0 \le i < t$, otherwise it factors N with probability $\frac{1}{2}$. In the first case continue the factoring algorithm as follows until it factors N with probability $\frac{1}{2}$:
Supplemental steps to the factoring algorithm. Repeat the entire algorithm using independent coin flips and construct independent pairs (Y, Z) with $Y^{2^t} = Z^{2^{t+\ell}} \bmod N$ until either of the following two cases arises.

Case I. $Y^{2^i} \neq -Z^{2^{i+\ell}}$ for all i with $0 \le i < t$ holds for some (Y, Z). Then terminate as the proposed factoring method succeeds using Y, Z with probability $\frac{1}{2}$.

Case II. $Y^{2^i} = -Z^{2^{i+\ell}}$ holds for two independent pairs $(Y, Z), (Y', Z')$. Then replace these pairs by $(Y_{\text{new}}, Z_{\text{new}})$ with $Y_{\text{new}} := YY'$, $Z_{\text{new}} := ZZ'$. If $Y_{\text{new}}^{2^{i_{\text{new}}}} = -Z_{\text{new}}^{2^{i_{\text{new}}+\ell}}$ holds for some i_{new} then we have $i_{\text{new}} < i$, otherwise terminate (as the proposed factoring method succeeds using $Y_{\text{new}}, Z_{\text{new}}$ with probability $\frac{1}{2}$).

Continue the repetitions of the entire algorithm using idependent coin flips and continue to decrease i until the algorithm either terminates in Case I or enters Case II with $i = 1$. In the latter case the proposed factoring method succeeds using $Y_{\text{new}}, Z_{\text{new}}$ with probability $\frac{1}{2}$, in particular $\{\gcd(Y_{\text{new}} \pm Z_{\text{new}}, N)\} = \{p, q\}$ holds with probability $\frac{1}{2}$.

With the supplemental steps the algorithm factorizes N with probability $\frac{1}{2}$. The supplemental steps increase the time bound for factoring by a factor $O(\ell)$. The correctness proof of the amended factoring method uses the following observation

We see from $Y^{2^t} = Z^{2^{t+\ell}} \bmod N$ that Z^{2^ℓ}/Y is a 2^t-root of $1 \bmod N$. This root is not necessarily uniformly distributed over all 2^t-roots of $1 \bmod N$. But it is uniformly distributed within certain cosets.

Fact. *Let $Y = Y(Z^{2^t})$ be a function of Z^{2^t} that solves $Y^{2^t} = Z^{2^{t+\ell}} \bmod N$ with $\ell < t$. Then Z^{2^ℓ}/Y takes the roots in $c_0 R_N(2^t)^{2^\ell}$ with equal probability for all $c_0 \in R_N(2^t)$, where $R_N(2^t)$ denotes the group of 2^t-roots of $1 \bmod N$ and $R_N(2^t)^{2^\ell} \subset R_N(2^t)$ denotes the subgroup of 2^ℓ-powers.*

All subsequent factoring algorithms in the paper have to be amended in the same way.