Let $n = 115792089237316195423570985008687907852837564279074904382605163141518161494337$.

Let $\lambda = 37718080363155996902926221483475020450927657555482586988616620542887997980018$.

Let $a_1 = 64502973549206556628585045361533709077$.

Let $b_1 = -303414439467246543595250775667605759171$.

Let $a_2 = 367917413016453100223835821029139468248$.

Let $b_2 = 64502973549206556628585045361533709077$.

Let $g_1 = 4227266874520800895210949532813473158086059$.

Let $g_2 = 1988456870492546948105835483415221103310491 4$.

Let $\boldsymbol{M} = \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}$.

Let $k \in \mathbb{Z}$ such that $0 \leq k < 2^{256}$.

Let $c_1 \in \mathbb{Z}$ such that $\left| c_1 - \frac{k\, g_1}{2^{272}} \right| \leq \frac{1}{2}$.

Let $c_2 \in \mathbb{Z}$ such that $\left| c_2 - \frac{k\, g_2}{2^{272}} \right| \leq \frac{1}{2}$.

Let $\varepsilon_1 = \frac{g_1}{2^{272}} - \frac{b_2}{n}$.

Let $\varepsilon_2 = -\frac{b_1}{n} - \frac{g_2}{2^{272}}$.

Let $k_1 = k - c_1\, a_1 - c_2\, a_2$. (Note, not modular arithemetic).

Let $k_2 = -c_1\, b_1 - c_2\, b_2$. (Note, not modular arithmetic)

Let $r_2 = k_2 \pmod{n}$.

Let $r_1 = k - r_2 \lambda \pmod{n}$.

The values of r_1 and r_2 should be the values returned by `secp256k1_scalar_split_lambda` when given k as input.

Lemma 1. $n | a_1 + b_1\, \lambda$

Lemma 2. $n | a_2 + b_2\, \lambda$

Lemma 3. $0 < \varepsilon_1, \varepsilon_2 < 2^{-273}$.

Lemma 4. $|\boldsymbol{M}| = n$.

Lemma 5. $\boldsymbol{M} \begin{pmatrix} \frac{k\, b_2}{n} \\ -\frac{k\, b_1}{n} \end{pmatrix} = \begin{pmatrix} k \\ 0 \end{pmatrix}$.

Lemma 6. $\left| c_1 - \frac{k\, b_2}{n} \right| < \frac{1}{2} + \frac{1}{2^{17}}$.

Proof.

$$
\begin{aligned}
& \left| c_1 - \frac{k\, b_2}{n} \right| \\
= & \left| c_1 - \frac{k\, g_1}{2^{272}} + \frac{k\, g_1}{2^{272}} - \frac{k\, b_2}{n} \right| \\
\leq & \left| c_1 - \frac{k\, g_1}{2^{272}} \right| + \left| \frac{k\, g_1}{2^{272}} - \frac{k\, b_2}{n} \right| \\
= & \left| c_1 - \frac{k\, g_1}{2^{272}} \right| + k |\varepsilon_1| \\
< & \frac{1}{2} + 2^{256}\, 2^{-273} \\
= & \frac{1}{2} + \frac{1}{2^{17}}
\end{aligned}
$$

$\square$

Lemma 7. $\left|c_2 + \frac{k\,b_1}{n}\right| < \frac{1}{2} + \frac{1}{2^{17}}$.

Proof.

$$\begin{aligned}
& \left|c_2 + \tfrac{k\,b_1}{n}\right| \\
= \;& \left|c_2 - \tfrac{k\,g_2}{2^{272}} + \tfrac{k\,g_2}{2^{272}} + \tfrac{k\,b_1}{n}\right| \\
\leq \;& \left|c_1 - \tfrac{k\,g_2}{2^{272}}\right| + \left|\tfrac{k\,g_2}{2^{272}} + \tfrac{k\,b_1}{n}\right| \\
= \;& \left|c_1 - \tfrac{k\,g_1}{2^{272}}\right| + k\,|-\varepsilon_2| \\
< \;& \tfrac{1}{2} + 2^{256}\,2^{-273} \\
= \;& \tfrac{1}{2} + \tfrac{1}{2^{17}}
\end{aligned}$$

$\square$

Lemma 8. $|k_1| < (a_1 + a_2)\left(\frac{1}{2} + \frac{1}{2^{17}}\right) < 216213492388562293480965471806682953052\,.$

Proof.

$$\begin{aligned}
& |k_1| \\
= \;& |k - c_1\,a_1 - c_2\,a_2| \\
= \;& \left|k\,\tfrac{a_1\,b_2 - a_2\,b_1}{n} - c_1\,a_1 - c_2\,a_2\right| \\
= \;& \left|\left(k\,\tfrac{b_2}{n} - c_1\right)a_1 - \left(k\,\tfrac{b_1}{n} + c_2\right)a_2\right| \\
\leq \;& \left|k\,\tfrac{b_2}{n} - c_1\right|a_1 + \left|k\,\tfrac{b_1}{n} + c_2\right|a_2 \\
< \;& \left(\tfrac{1}{2} + \tfrac{1}{2^{17}}\right)a_1 + \left(\tfrac{1}{2} + \tfrac{1}{2^{17}}\right)a_2 \\
= \;& (a_1 + a_2)\left(\tfrac{1}{2} + \tfrac{1}{2^{17}}\right) \\
< \;& 216213492388562293480965471806682953052
\end{aligned}$$

$\square$

Lemma 9. $|k_2| < (b_2 - b_1)\left(\frac{1}{2} + \frac{1}{2^{17}}\right) < 183961513495325369486767030355733591695\,.$

Proof.

$$\begin{aligned}
& |k_2| \\
= \;& |-c_1\,b_1 - c_2\,b_2| \\
= \;& \left|k\,\tfrac{b_1\,b_2 - b_2\,b_1}{n} - c_1\,b_1 - c_2\,b_2\right| \\
= \;& \left|\left(k\,\tfrac{b_2}{n} - c_1\right)b_1 - \left(k\,\tfrac{b_1}{n} + c_2\right)b_2\right| \\
\leq \;& \left|k\,\tfrac{b_2}{n} - c_1\right|(-b_1) + \left|k\,\tfrac{b_1}{n} + c_2\right|b_2 \\
< \;& \left(\tfrac{1}{2} + \tfrac{1}{2^{17}}\right)(-b_1) + \left(\tfrac{1}{2} + \tfrac{1}{2^{17}}\right)b_2 \\
= \;& (b_2 - b_1)\left(\tfrac{1}{2} + \tfrac{1}{2^{17}}\right) \\
< \;& 183961513495325369486767030355733591695
\end{aligned}$$

$\square$

Lemma 10. $r_1 \equiv k_1 (\operatorname{mod} n)$.

Proof.

$$
\begin{aligned}
& r_1 \\
\equiv\ & k - r_2\lambda \\
=\ & k + c_1\, b_1\, \lambda + c_2\, b_2\lambda \\
\equiv\ & k + c_1\, b_1\, \lambda - c_1\, (a_1 + b_1\, \lambda) + c_2\, b_2\lambda - c_2\, (a_2 + b_2\, \lambda) \\
=\ & k - c_1\, a_1 - c_2\, a_2 \\
=\ & k_1
\end{aligned}
$$

$\square$

Theorem 11. $0 \leq r_1 < 2162134923885622934809654718066829530\!52$

or

$n - 216213492388562293480965471806682953051 \leq r_1 < n.$

Theorem 12. $0 \leq r_2 < 183961513495325369486767030355733591695$

or

$n - 183961513495325369486767030355733591694 \leq r_2 < n.$