Implementierung

- elliptische Kurven Arithmetik

  $P+Q$ auf E

  $\underbrace{P+P+\dots+P}_{k \cdot P}$ vorzugsweise mit der Beschleunigung SQUARE-AND-MULTIPLY (hier: DOUBLE-AND-ADD)

- Eingabe mehrere Varianten

  a) wähle u, v probiere alle $|D|$, ob eine Primzahl p mit $u^2 + |D|v^2 = 4p$ existiert

  b) wähle p, berechne $4p$, löse für alle $|D|$ die Gleichung $4p = u^2 + |D|v^2$ nach u, v

  [benutze $u^2 + |D|v^2 \equiv 0 \bmod p$

  $\Rightarrow u^2 \equiv -|D|v^2 \bmod p$

  $\Rightarrow \frac{u^2}{v^2} \equiv -|D| \bmod p$

  $\Rightarrow \left(\frac{u}{v}\right)^2 \equiv -|D| \bmod p$

  $\rightarrow$ Quadratwurzel mod p]

  c) wähle D, probiere Werte u, v so dass

  $$u^2 + |D|v^2 \equiv 0 \bmod 4$$

  und $p = \frac{u^2 + |D|v^2}{4}$ eine Primzahl ist

y	$y^2 \bmod 4$
0	0
1	1
2	0
3	1

Quadratischer Nichtrest

return g, falls ja

Parameter a, b aus den Fällen

$D=-3$, $D=-4$, $D \notin \{-3,-4\}$

6 Kurven, 4 Kurven, 2 Kurven

$|E| \in \{p+1+u, p+1-u, \dots\}$

Zuordnen der Parameter zum richtigen $|E|$-Wert:

- für mögliche $|E|$-Werte teste
  $|E| \cdot P = \mathcal{O}$ für zufälligen Punkt $P \in E$
- gibt es nur eine Kurve (a,b) mit dieser Eigenschaft, dann ist eine Zuordnung gefunden.

Zufälliger Punkt:

$y^2 \equiv x^3 + ax + b \mod p$

x wählen, teste ob $x^3+ax+b \mod p$ ein Quadrat ist

$(x^3+ax+b)^{\frac{p-1}{2}} \equiv 1 \mod p$

danach Quadratwurzel aus $x^3+ax+b \mod p$

$\rightarrow y \rightarrow$ Punkt $P=(x,y)$