Zufallszahlen mit elliptischen Kurven

dual EC - DRBG [nicht verwenden]

E elliptische Kurve mod p Primzahl

$P, Q \in E$ zwei zufällige Punkte

[im Standard nicht zufällig gewählt]

$s = SHA(\ldots)$

$t = s \oplus \ldots$ → frei wählbar (seed)

$s = (t \cdot P)_x$ x-Koordinate von $t \cdot P$

$r = (s \cdot Q)_x$ → Output $r \bmod 2^l$

$t = s$

l Bits Zufallszahlen

Parametergrößen:

Bitlänge von $\lvert E \rvert$ bzw. p	256	384	521
Output-Bits l	240	368	504

Attacke: wenn der Angreifer den Zusammenhang $Q = k \cdot P$ kennt:

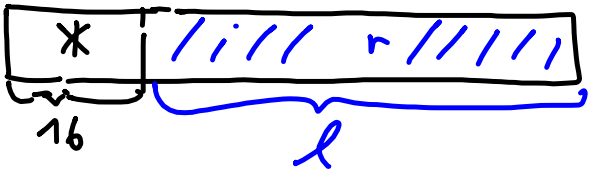
kann er den Datenstrom vorhersagen

Details:

$Q = k \cdot P$

beobachte 240 Bit r

diese stammen aus $(s \cdot Q)_x$



$\Rightarrow$ kann alle diese x-Werte (r_i) aufzählen

$0 \leq i \leq 2^{16} - 1$ maximal

typischerweise haben 50% der x-Werte zwei y-Werte, d.h. $\approx 2^{15}$ r_i-Werte und damit $\approx 2^{16}$ zugehörige Punkte

$R_i = (r_i, \pm y_i)$

$\pm y_i$ kommen im EC-DRBG nicht vor $\rightarrow$ irrelevant

Würde man

$$R = s \cdot Q$$

nach s auflösen können (schwer, ECDH / ECDSA)

hätte man aus 2^{15} möglichen R_i

nun 2^{15} mögliche $s_i \rightarrow 2^{15}$ mögliche k_i

→ diese Liste kann mit den nächsten ℓ Output bits abgeglichen werden