

ECDH Diffie-Hellman

Regeln: $A: z \in \mathbb{Z} \times \xrightarrow{\text{Kurve } x \text{ -Kurve}}$ $\left\{ \begin{array}{l} \text{Oberschicht} \\ \text{Kurve-Kurve} \end{array} \right.$
 $B: w \in \mathbb{Z} \times \xrightarrow{\text{Kurve } y \text{ -Kurve}}$

Nöcher se unterchung v. Kugel gruppe G
 Gruppe G je Kugel, charakter g Kugel $P(x)$
 multiplikation Notace $g \times$
 addition Notace $[x]P$ $[x]x$

Vel. Kugel v. DLP starke Kugel "deten"
 $Q = [x]P \xrightarrow{?} w \in \mathbb{Z} \times$ se 2 Kugel
 $Q \text{ a } P$

A i B mají společné (C, P)

A si vybere klíč d_A $A \xrightarrow{[d_A]P} B : [d_B][A]P$

B si vybere klíč d_B $B \xrightarrow{[d_B]P} A : [d_A][d_B]P$

Oba mají $d_A d_B P$, což je sdílená
 $d_A d_B = d_B d_A$ tajemství

$$[d_A d_B](P) = \left(\begin{matrix} 6 \\ 17 \end{matrix} \right)$$

ZA KLÍČ SE BERE
POUZE $\{$



Symmetric

RSA a DHP modp

ECC

80

1024

160

Order

112

2048

224

128

3072

256

144

7680

384

256

15360

521

Elegant kryptosystém

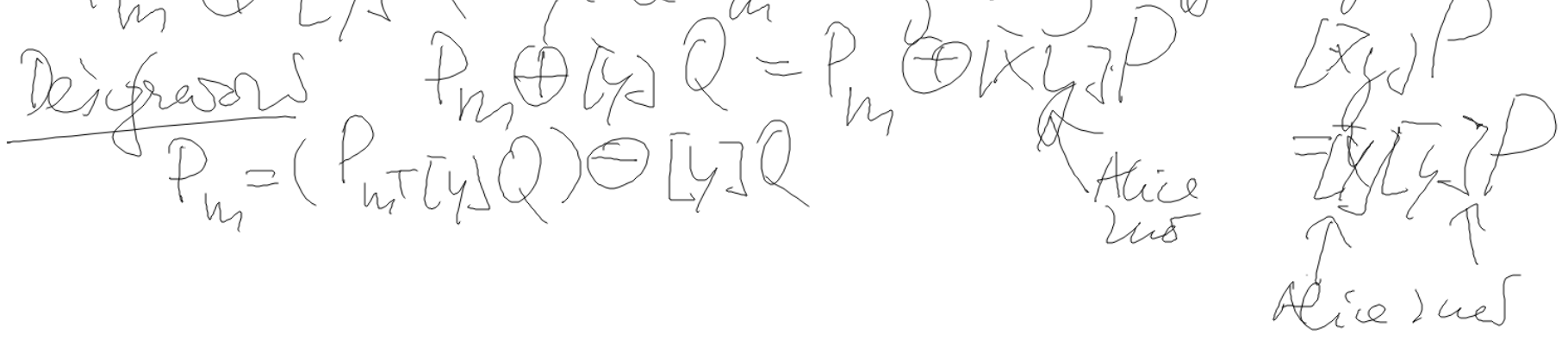
Alice (C, P, Q) $Q = [x]P$ x tajemství

Bob zvolí y a vypočítá a pole $[y]Q$

Oba mají $[xy]P$, a to se používá pro dešifrování

Všobu zprávu m pole Bob jako

$P_m \oplus [y]Q$ kde P_m bod křivky vyjadřující m



ECDSA

Elliptic curve digital signature algorithm

Alice overetuje (C, P, P, Q, g) $g: C \rightarrow \mathbb{Z}$

P řád cyklické grupy generované P

$$Q = [x]P \quad x \text{ tajemství Alice}$$

Alice podepisuje, Bob overuje

$m \in \mathbb{Z}$ vybraná náhodně $y, 1 \leq y < P$

posílá se $(m, [y]P, y^{-1}(m + xg([y]P)) \bmod P)$

~~overuje~~ $(a) = m (y^{-1}(m + xg([y]P)))^{-1} \bmod P$

$$y \cdot \frac{m}{m + xg([y]P)}$$

$$(b) = g([y]P) (y^{-1}(m + xg([y]P)))^{-1} = y \frac{g([y]P)}{m + xg([y]P)}$$

$$[a + xb]P = [y]P$$

" $[a]P + [b]P = [a]P + [b]P$ "