Diffie-Hellman su curve ellittiche

Alice e Bob scelgono una curva ellittica prima $E_p(a, b)$ e un punto $B \in E_p(a, b)$ di ordine n elevato (sostituisce il generatore; se l'ordine è basso lo è il periodo di kB)

Alice	**Eve**	**Bob**
concorda a, b, p, B con Bob	intercetta a, b, p, B	concorda a, b, p, N con Alice
sceglie a caso $1 < n_A < n$		sceglie a caso $1 < n_B < n$
invia $P_A = n_A B$	intercetta P_A	riceve P_A
riceve P_B	intercetta P_B	invia $P_B = n_A B$
calcola $k = n_A P_B$		calcola $k = n_B P_A$

Vale:

$$k = n_A P_B = n_A n_B B = n_B n_A B = n_B P_A,$$

quindi Alice e Bob hanno la stessa chiave k, mentre Eve può ottenerla solo se riesce a ricavare n_A o n_B, e questo richiede di risolvere un logaritmo discreto su curve ellittiche, che ha costo esponenziale (più difficile del problema equivalente in aritmetica modulare).

Da k si possono estrarre 256 bit per formare una chiave AES.

È vulnerabile ad attacchi man-in-the-middle.