Forward secrecy

Proprietà di alcuni protocolli di scambio di chiavi per cui è garantito che le chiavi di sessione generate non possono essere compromesse nel caso in cui un attaccante venga in possesso di chiavi a lungo termine.

I cifrari ibridi non garantiscono forward secrecy: se l'attaccante memorizza lo scambio e in un secondo momento riesce ad ottenere la chiave privata, può usarla per decifrare la chiave simmetrica scambiata e riuscire a leggere tutte le comunicazioni. I parametri segreti di Diffie-Hellman (gli esponenti del generatore) vengono invece gettati dopo la generazione delle chiavi, perciò non ci sono valori che devono essere mantenuti segreti a lungo e che potrebbero essere scoperti.