Mode of Operation	Invertierbarkeit von F?	c-Text-Expansion	Vorberechnungen?	Parallelisierbar?
CBC	ja, PRP	*(l + 1) / l*	nein	Ja, Entschlüsselung kann parallelisiert werden, denn jeder Block kann selbstständig entschlüsselt werden. Warum? Weil man IV, c_i und F_k^{-1} hat: bei der Decryption wird unabhängig von anderen Blöcken geXORt .
OFB	nein, PRF	*(l + 1) / l*	Ja, der Keystream kann mithilfe von IV und F_k vorberechnet werden. Weil die F_k immer vor dem Xor verwendet wird und somit unabhängig von m ist.	Eher schwierig: nur wenn vorberechnet wird. Das XOREn am Schluss ist eventuell parallelisierbar…
CTR	nein, PRF	*(l + 1) / l*	Ja, IV kann im Vorhinein hochgezählt werden. Zudem kann der IV-Counter für weitere Vorberechnung in F_k gesteckt werden.	Ja sowohl Entschlüsselung und Verschlüsselung: hier sind die Blöcke sehr unabhängig. Sie sind nicht mehr an Berechnungen von vorherigen Blöcken gekoppelt. Stark parallelisierbar. Nicht nur das XORn, sondern der ganze Block, sofern der Counter vorhanden ist.