

Fluhrer–McGrew biases in initial keystream bytes

