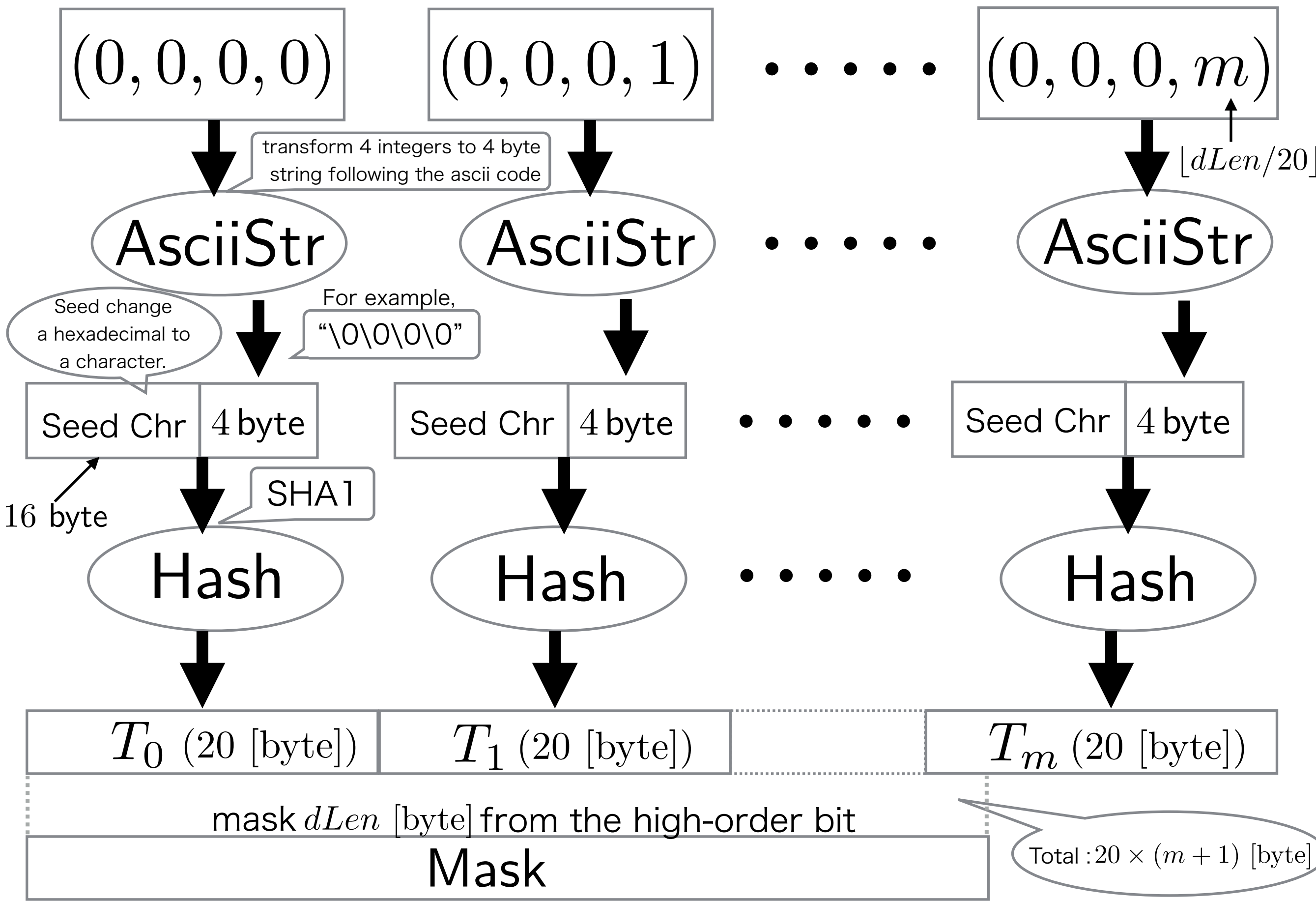
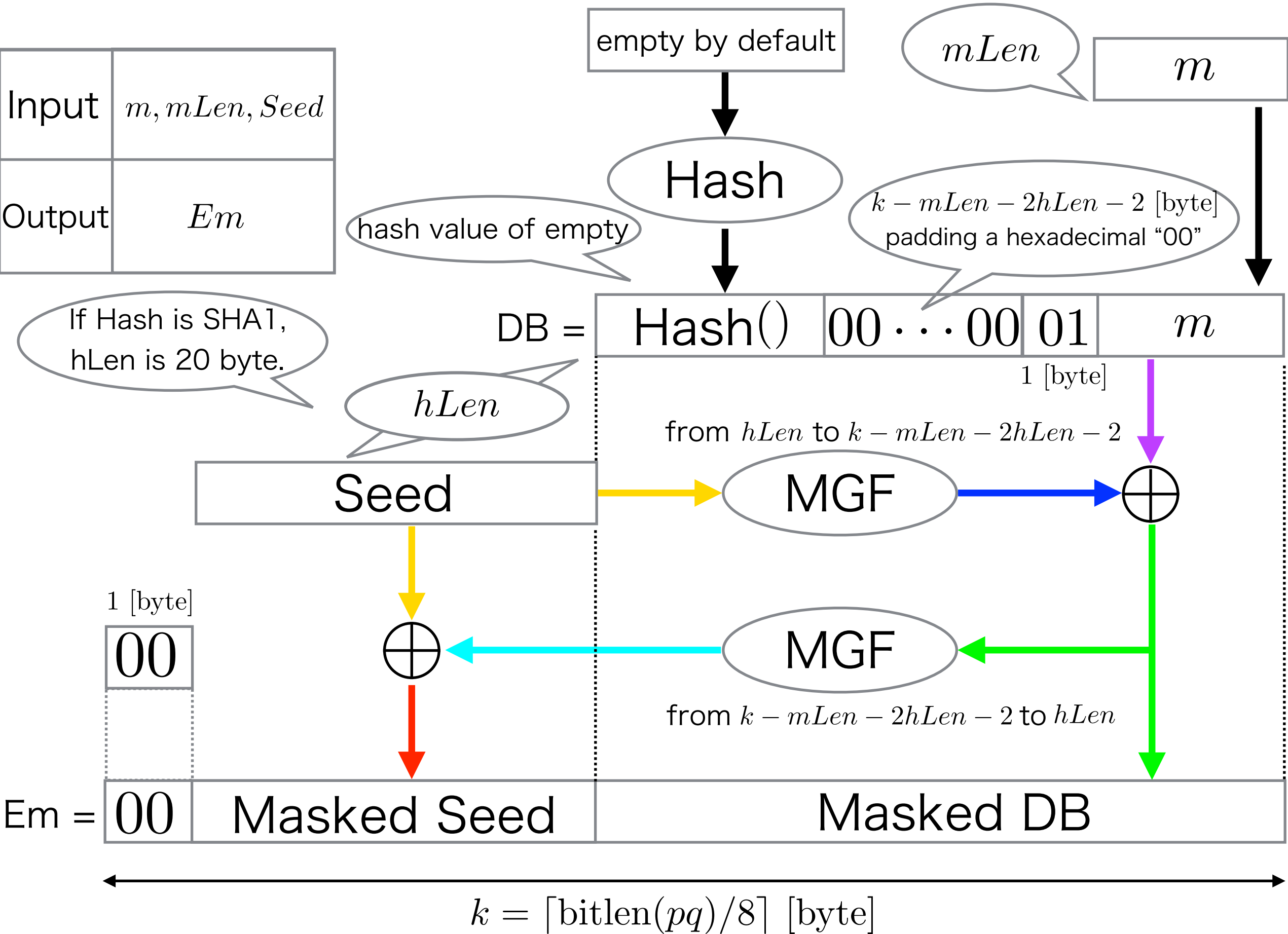


MGF(Masked Generation Function) (Input : Seed, dLen → Output : Mask)

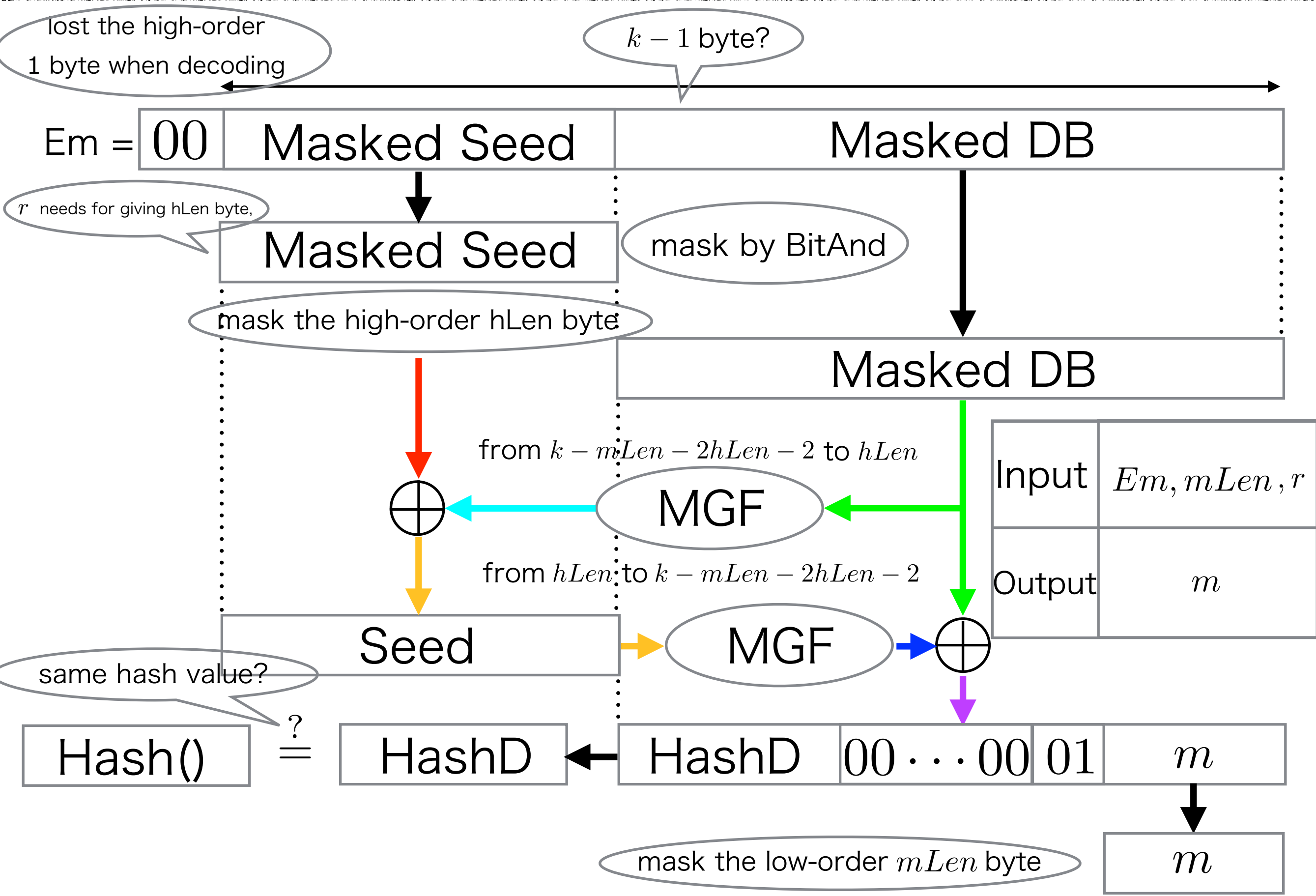


# Padding of RSA-OAEP Encode

Input	$m, mLen, Seed$
Output	$Em$



# Reverse Padding of RSA-OAEP Decode



# RSA-PSSの署名生成のパディング処理について

