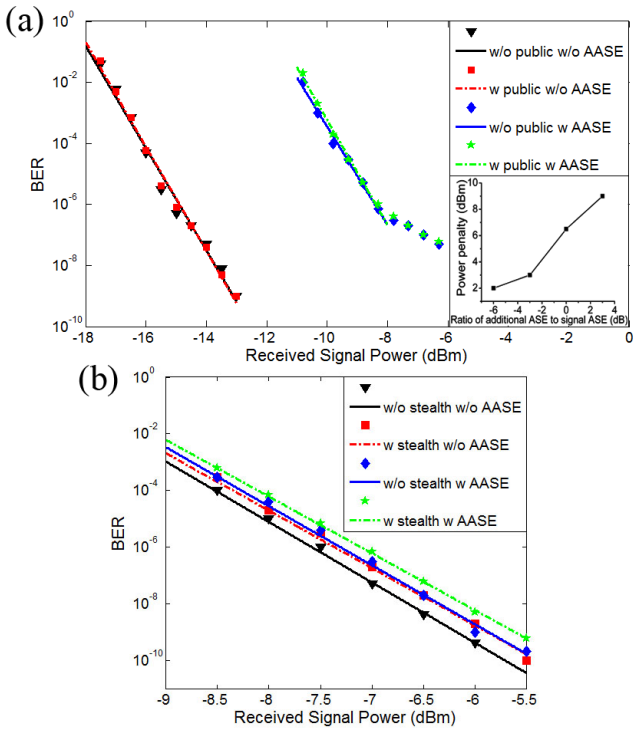

Fig. 5. BER performance versus received signal power for: (a) the stealth channel with and without public channel and AASE, data after the noise floor is not considered in the linear fit with AASE. The inset shows the penalty from additional ASE at different ratio of addition ASE to signal ASE. (b) The public channel with and without the stealth channel and additional ASE.

4. Conclusion

An optical steganography method is proposed and experimentally demonstrated using ASE noise and homodyne detection. ASE noise carrying a stealth signal has the same spectrum as the ASE noise originally existing in the system, which hides the stealth signal in the frequency domain. In the time domain, because the ASE noise has a short coherence length, the optical delays must be matched exactly in order to receive the stealth signal. Changing the delay length frequently makes it impossible for the eavesdropper to find and track the optical delay length difference. BER measurements of the system show that the stealth channel and the public channel do not interfere with each other. Furthermore, the public channel does not induce any power penalty on the stealth channel. On the other hand, the stealth channel only causes a 0.2-0.3 dBm power penalty on the public channel.

Acknowledgment

The authors would like to thank John Chang and Matt Chang in the Lightwave Communications Laboratory at Princeton University for help with lab and equipment maintenance.

#178601 - $15.00 USD Received 31 Oct 2012; revised 2 Jan 2013; accepted 3 Jan 2013; published 18 Jan 2013