transmission distance without the dispersion compensation. We experimentally measured that if the DCF is not used, the dispersion from 25km standard single mode fiber (SSMF) expends the sharp rising edge of a signal to one with 3ns rising. By using the criterion $B\Delta T<1$, where B is the data rate of the phase mask, which is 4Gb/s, the time delay (ΔT) caused by the dispersion has to be less then 250ps. Considering both the rising edge and the falling edge, the system can only tolerate uncompensated dispersion from 1km SSMF. Although this limits resilience of this system in a dynamic network, the precise requirement of dispersion compensation can actually provide another layer of security. We have demonstrated that the dispersion can expend the key space for optical steganography [8].

Besides dispersion, the wide optical spectrum of ASE noise also limits the signal to noise ratio for long distance transmission. When an optical amplifier is used to amplify the signal in a traditional long distance communication system, an optical filter is deployed to remove the ASE noise from the optical amplifier. However, if ASE carries the signal, the optical filter cannot be used. The ASE carrying signals cannot be separated from the new generated noise ASE.

The ASE also has wide band radio frequency noise, which protect the phase mask from being detected. As a tradeoff, the wide band radio frequency noise limits the data rate of both the stealth channel and the phase mask. The stealth channel with a higher data rate is accompanied with more ASE noise. Our experiment shows that the BER increase while the stealth channel date rate increases [Fig. 7]. The data rate of the phase mask is designed to be high enough so that the ASE noise with the same bandwidth accompanied can protect the phase mask data from being detected. However, the data rate of the phase mask cannot be too high because the receiver needs to temporally overlap the received phase mask with the recovery phase mask. If the phase mask is accompanied by more noise, it will degrade the recovery process and cause more power penalty.

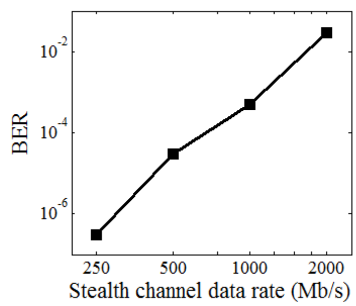

Fig. 7. Measurement of BER for different stealth channel data rates.

4. Conclusion

We have proposed and experimentally demonstrated a phase mask encryption method to cover stealth data bits and protect the security of the stealth channel. The phase mask is implemented by imposing phase modulation on the ASE noise, and can be easily changed by using different codes in the phase modulation. The phase mask code itself is protected by the wideband noise from the ASE, which is designed to be 16 times stronger than the noise in the stealth data. More than 18,000 codes are available for the phase mask. Without knowing the right phase mask code to recover the signal, the received signal has its amplitude reduced to less than 25% of its original value, in addition to having a randomized phase. Furthermore, the phase mask introduces only a 0.3 dBm power penalty to the stealth channel.

Acknowledgment

The authors would like to thank Yue Tian and John Chang in the Lightwave Communications Research Laboratory of Princeton University for their assistance. We are also grateful for the helpful comments of the reviewers.