FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

TECHNISCHE FAKULTÄT

Elektrotechnik-Elektronik-Informationstechnik

# EEI KOLLOQUIUM

## Error Free Perfect Secrecy Systems

**Dr. Siu-Wai Ho**
Senior Research Fellow, University of South Australia, Adelaide

**Montag, der 15.07.2013, $17^{00}$ Uhr**
Cauerstraße 7, Raum N5.15

**Diskussionsleitung: Prof. Dr.-Ing. J. Huber**

Shannon's fundamental bound for perfect secrecy stated that the entropy of the secret message U cannot be larger than the entropy of the secret key R shared by the sender and the legitimated receiver. Massey gave an information-theoretic proof of this result and the proof did not require U and R to be independent. By adding an extra assumption that I(U;R) = 0, we show a tighter bound on H(R) in this talk. Our bound states that the logarithm of the message sample size cannot be larger than the entropy of the secret key. We also consider the case that a perfect secrecy system is used multiple times. A new parameter, namely expected key consumption, is defined and justified. We show the existence of a fundamental trade-off between the expected key consumption and the number of channel uses for transmitting a cipher-text. A coding scheme, which is optimal for minimizing the expected key consumption, is introduced.