Secret key generation from correlated randomness

One-time pad

Crypto for the truly paranoid

- no reliance on unproven assumptions
  - e.g. factoring, discrete logarithms
- information-theoretic proof of security

The one-time pad (OTP)

- n-bit message X
- n-bit secret key K, uniformly random
- encryption: ciphertext $C = X \oplus K$
- decryption: $C \oplus K = X$
- use key only once!

Security of the one-time pad

ciphertext: $C = X \oplus K$

decryption: $C \oplus K = X$

$$H(X \mid C) = H(C \oplus K \mid C) = H(K) = n.$$

- Eavesdropper sees C
  - has to guess X knowing only C
- Ignorance about X is n bits
  - *which is also the message length!*
- Any message equally likely

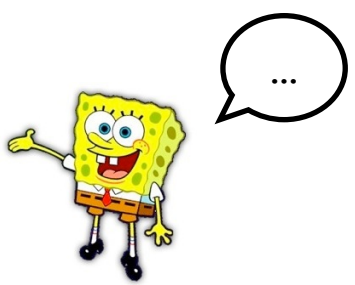
Conditions for perfect security

More generally:

- $H(X|C) = H(\text{Dec}(K,C)|\ C\ ) \leqslant H(K)$
  - for perfect security, we demand $H(X|C)$ to be $H(X)$
- Ergo: perfect security only possible if $H(K) \geqslant H(X)$.

So, what if $H(K) < H(X)$ and you want perfect security?

Drat!



Noise comes to the rescue

"No go theorem":

- Perfect security impossible when $H(K) \leqslant H(X)$.

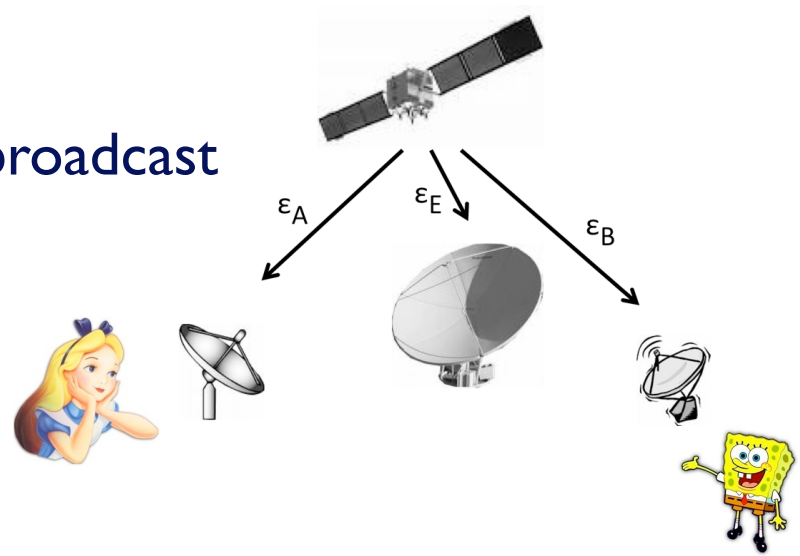
But there are hidden assumptions!

- Eve's eavesdropping is assumed 100% accurate.

Maurer 1993

Two Realistic (=pessimistic) scenarios

1. Noisy broadcast channel
   - Bob and Eve have noisy reception of Alice's broadcast
   - Eve may have best reception
2. Satellite scenario
   - three noisy channels.
   - Eve may have best reception.



Scenario 1: noisy broadcast

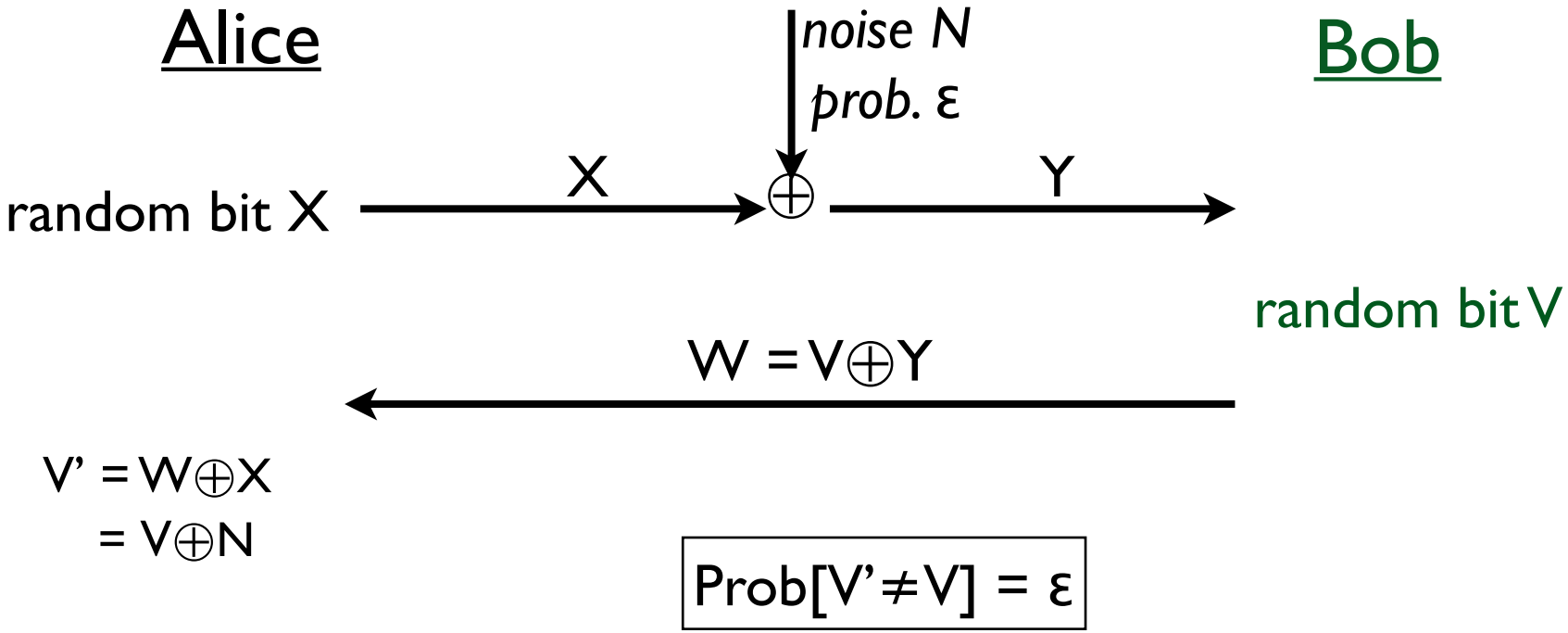
Basic idea

- somehow create noisy conceptual channel Bob→Alice
  - Eve's noise becomes worse than A&B's
- then create shared secret
  - exploit Eve's ignorance caused by noise

For simplicity: The Binary Symmetric Channel (BSC)

- definition of a BSC
  - binary symbols 0/1
  - independent noise for each bit separately
  - bit flip probability does not depend on 0/1 value
- all channels will be modeled as BSC

Scenario 1; making a virtual channel



Eve

receives Z = X⊕D,
D independent of N.
Bit flip prob. δ.

$V_E = Z \oplus W$
$= V \oplus (N \oplus D)$

$\text{Prob}[V_E \neq V] = \varepsilon * \delta$

BSC concatenation

Scenario 1; using the virtual channel

Virtual channel from Bob to Alice:

- Alice has error rate ε
- Eve has error rate $\varepsilon * \delta > \varepsilon$

The trick:

- Bob picks random message M;
  sends encode(M) over the virtual channel
- Code parameters specially chosen
  - error rate ε can be corrected
  - error rate $\varepsilon * \delta$ cannot
  - Eve learns (almost) nothing about M

Scenario 1; general theorems

Noisy Broadcast without public discussion

Theorem 4.6 *The secrecy capacity of the above described noisy broadcast channel (BSC with error rates ε and δ) is*

$$C_{\mathrm{s}}(\varepsilon,\delta) = \begin{cases} h(\delta) - h(\varepsilon) & \text{if } \delta > \varepsilon \\ 0 & \text{otherwise} \end{cases}$$

Noisy Broadcast with public discussion

Theorem 4.8 *The secrecy capacity with public discussion of the described binary symmetric broadcast channel with error rates ε, δ is given by*

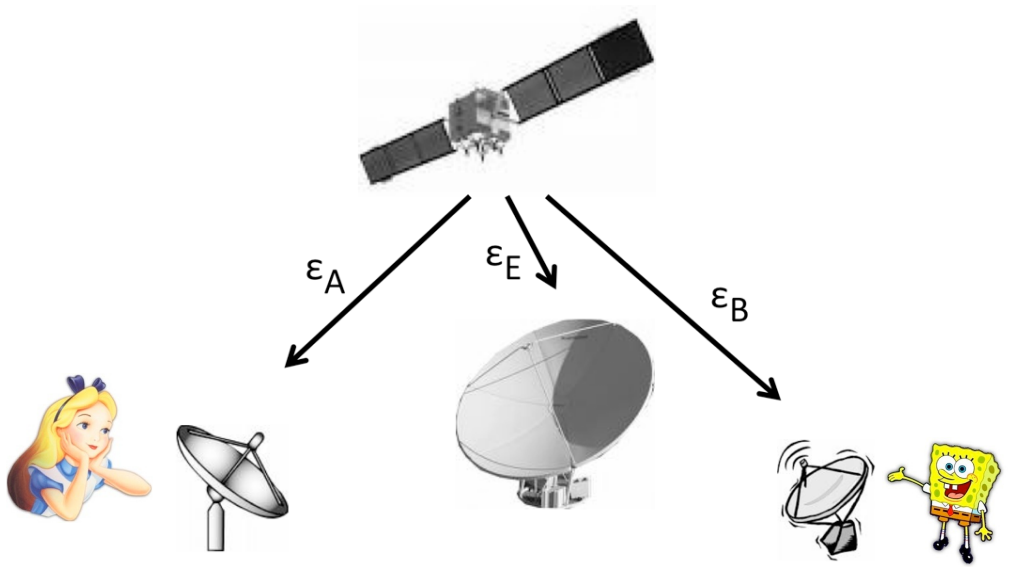
$$\widehat{C}_{\mathrm{s}}(\varepsilon,\delta) = h(\varepsilon * \delta) - h(\varepsilon).$$

Public discussion enables creation of the virtual channel !

Scenario 2; noisy satellite broadcast

Basic idea

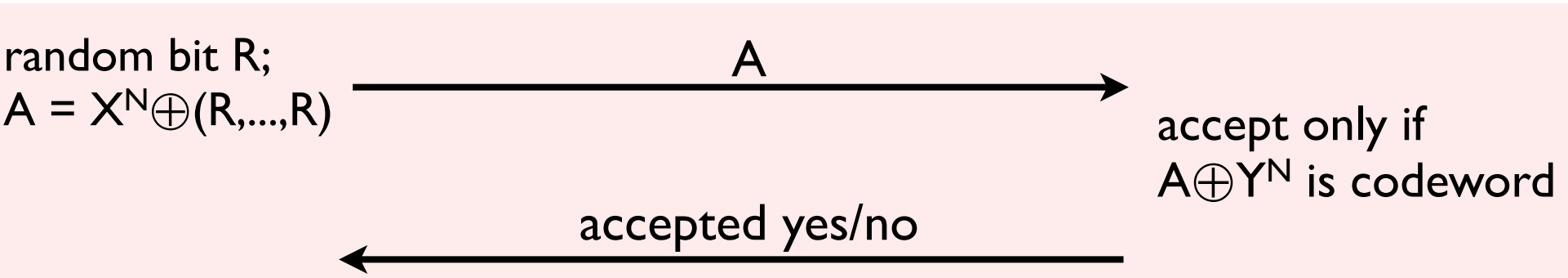
- Alice and Bob use public discussion and ECC
  - select low-noise bits
  - Eve has independent noise
  - virtual channel
- Tweak the parameters so that Eve has more noise than A&B on the virtual channel



Scenario 2; making the virtual channel

Example: repetition code

Alice (X) Bob (Y)



Virtual channel: Only look at the Accept events. Alice has sent bit R to Bob

$$p_{\rm ok} = (1 - \varepsilon_{\rm A} * \varepsilon_{\rm B})^N, \quad p_{\rm error} = (\varepsilon_{\rm A} * \varepsilon_{\rm B})^N, \quad p_{\rm accept} = p_{\rm ok} + p_{\rm error}$$

Error rate: $\beta = p_{\rm error}/p_{\rm accept}$

Eve has A and Z^N. Finding her error rate requires some lengthy analysis.

Scenario 2: Quality of the virtual channel

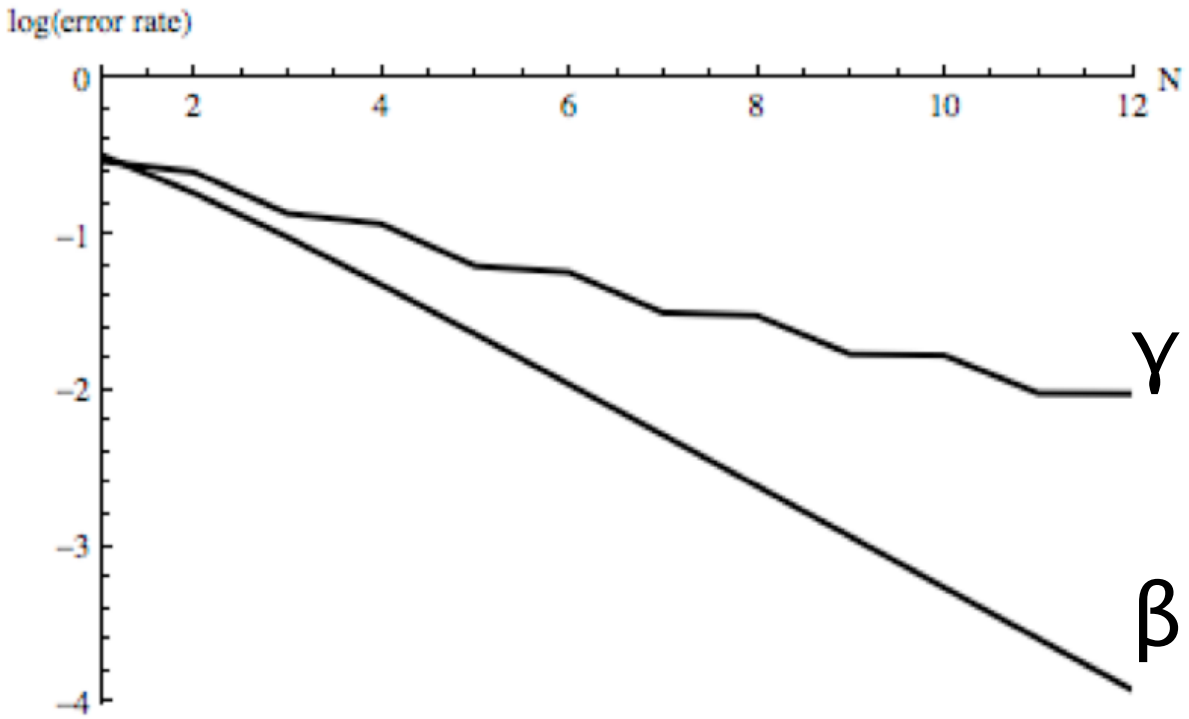


Figure 4.3: *Error rates β (lower curve) and γ (upper) as a function of N, for $\varepsilon_{\mathrm{A}} = \varepsilon_{\mathrm{B}} = 0.2$ and $\varepsilon_{\mathrm{E}} = 0.15$.*

Public discussion enables creation of the virtual channel !

Use the channel as in scenario 1