COMP-649A 2005 Homework set #1

Due Tuesday October, 4 2005 in class at 14h35

A. ISBN code

The **ISBN** numbers (codewords) that we find on all books originate from a code over $\mathbf{F_{11}}$ with alphabet **{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X }** where "**X**" stands for 10. This code is linear and its parameters are $\mathbf{[10,k,d]_{11}}$.

[10%] **1)** Use a bunch of books and determine the generating matrix of this code (provide the book titles and **ISBN** numbers that you used). Determine the values of **k** and **d** for this code.

[5%] **2)** For extra credit, find the smallest number of books that have linearly dependant ISBN numbers (provide the book titles and ISBN numbers that you used).

[10%] **3)** Show that the **ISBN** code has the extra property that for any **ISBN** codeword $\mathbf{a=(a_1,a_2,\ldots,a_{10})}$ if $\mathbf{a_i}$ and $\mathbf{a_j}$ are distinct symbols then the word $\mathbf{w=(w_1,w_2,\ldots,w_{10})}$ is never a codeword, where $\mathbf{w_k=a_k}$ for **k=1,2,3,…,10** except for **k=i,j** where instead $\mathbf{w_i=a_j}$ and $\mathbf{w_j=a_i}$.

B. BB84 channels

Let Alice and Bob share a random variable **W** uniformly distributed over all n-bit strings. Assume Eve, the eavesdropper is allowed to choose to see each bit of **W** through one of the following channels, parameterized by angle **@**

$$\mathbf{V_i} = \begin{cases} \mathbf{BSC_{\sin^2(@)}(W_i)} & \text{with probability } ½ \\ \mathbf{BSC_{\sin^2(\pi/4-@)}(W_i)} & \text{with probability } ½. \end{cases}$$

Moreover, Eve knows for each bit which of the two possibilities actually occurred. We have seen in class the extreme cases where **@=0** and where $\mathbf{@=\pi/8}$.

[15%] Show that the value of **@**, $\mathbf{0 \le @ \le \pi/8}$, which is most resistant to privacy amplification is **@=0**.

C. Uniformity, 3basis-BB84, and mutual identification

Let **C** be an **[n,k,d]** linear code over $\mathbf{F_q}$ with an **[n,n-k,d']** dual. Let $\mathbf{c=(c_1,c_2,\ldots,c_n)}$ be a randomly uniform codeword from **C**. Let $\mathbf{i_1,i_2,\ldots i_L}$ be a sequence of **L** distinct indices such that $\mathbf{1 \le i_j \le n}$.

[10%] **1)** Find and prove what is the smallest number of indices **L** (as a function of **n,k,d,d'**) for which the sub-word $\mathbf{(c_{i1},c_{i2},\ldots,c_{iL})}$ is not necessarily uniformly distributed (when **c** is uniform).

In the **BB84** protocol, Alice and Bob use two *conjugate* basis, rectilinear and diagonal, that are such that encoding and decoding in the same basis produce a noiseless channel, while encoding and decoding in the opposite basis yield a zero capacity channel.

[10%] **2)** Show existence of yet another basis that is conjugate to both rectilinear and diagonal.

Consider the problem for Alice and Bob, who share a ternary key **K,** to check that they have indeed the same key. Assume Alice is only able to send 3basis-BB84 coded bits and Bob is only able to measure them according to these 3 basis.

[20%] **3)** Device a protocol such that if Alice and Bob use the same key **K** then they will conclude so very fast, whereas if Alice is using **K** while Bob is using a random key **K'** they will only find out that **K≠K'** and no specific details except for the fact that roughly 2/3 of the trits are different.

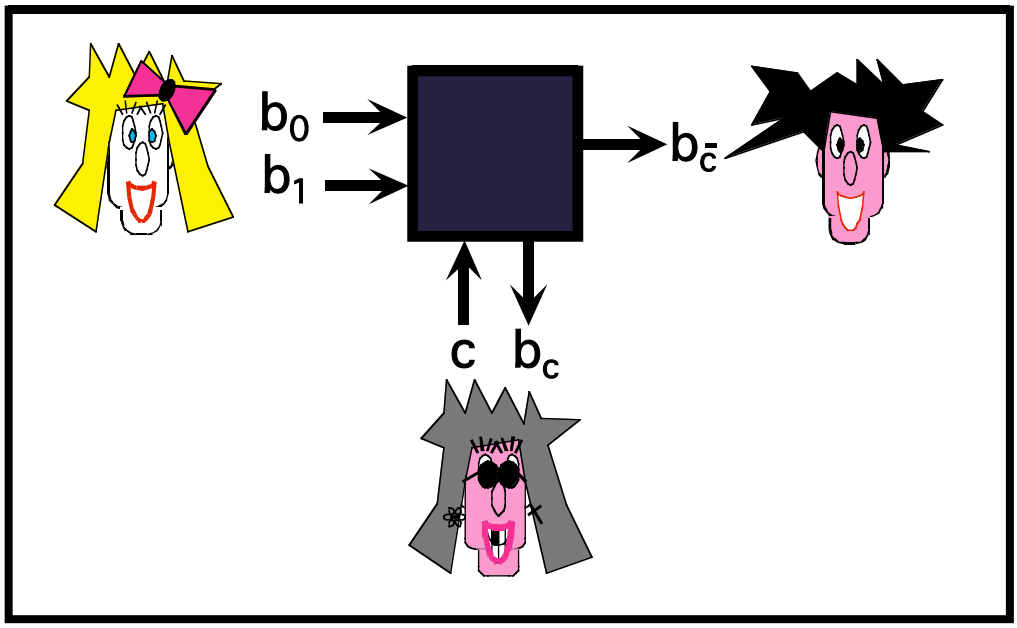
[5%] **4)** Explain why we can't use binary keys **K**.

…more on back

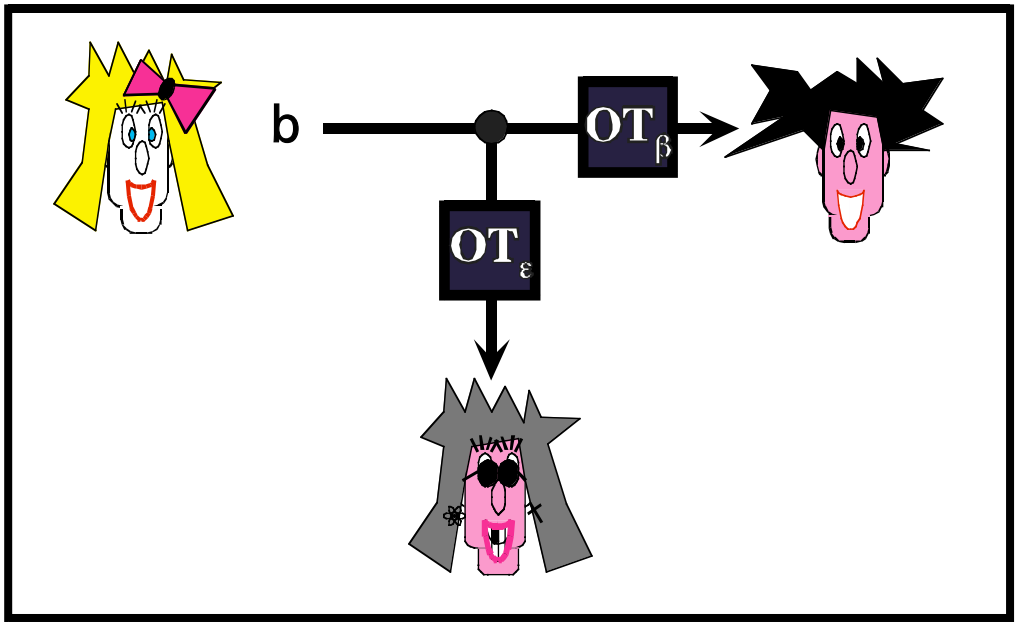
D. Chunnels

For each of the following situations, show how the honest Alice and Bob (who have access to an authenticated public channel) can take advantage of the insecure communication channel to exchange a secret key unknown to the eavesdropper Eve:

[10%] **1)**



[10%] **2)** Here, the probabilities β and ε of transmitting a bit are arbitrary (but fixed and known to everybody) and the OTs are independent.



…more on back