says that one bit will be wasted in all cases, so a natural question is how significant is this loss of channel capacity. It is easy to verify directly that p = 421 is the smallest prime for which two bits are unavailable. This problem, however, is of academic interest only, since a number theoretic calculation shows that no prime with fewer than 71 decimal digits can lose as many as three bits and that the prime would have to have 7777 decimal digits in order for four bits to be unavailable! The conclusion is that for realistic sized primes only a bit or two out of the ℓ bits total will be unavailable for subliminal communications.

A somewhat more serious (practical) problem is that there is no natural encoding/decoding between a space of binary messages and the elements of M_p. As we've seen, we can only encode k for which (k,p-1) = 1 for communication in the subliminal channel, but we must have a practical way to associate these values of k with the messages we wish to convey, which is easy for both the T_X and the S_X to use. For large primes, and especially for primes for which p-1 has several factors, this is so difficult to do that it limits the potential usefulness of the subliminal channel.

The next most important problem—in increasing order of significance—is the fact that some messages that can be encoded for communication in the subliminal channel are infeasible for the S_X to recover. Depending on the factorization of p-1, this may be a serious problem (because of the number of messages that can't be conveyed to the S_X) or a problem of only academic interest as is the case when p = 2p'+1 where there is only a single message that can't be recovered by the S_X. It should be pointed out, however, that this "lost message" isn't fixed by the choice of x so it can't be avoided by the coding scheme, rather for any choice of the message m, and hence of h, and of x, there will be one message whose encoding will be infeasible for the S_X to recover. For primes not of the special form p = 2p'+1, the preceding comments apply to a larger set of messages.

Finally, there is the most serious deficiency of all; namely, that the S_X must know the T_X's secret key, x, in order to recover the subliminal messages. This, of course, makes it possible for the S_X to utter indetectable forgeries of the T_X's signature. While there are real-world situations in which the T_X and the S_X trust each other unconditionally, or in which the T_X is willing to accept the risk of impersonation by the S_X to realize the benefit of subliminal communications—in general this is an unacceptable situation.