the S_X, is totally unable to detect the use of the subliminal channel since k" is equally likely to be any element of M_p; i.e., k" is indistinguishable from a session key, k, chosen from the elements of M_p with a uniform probability distribution. This follows from the unconditionally security of the Vernam encryption. The subliminal channel is therefore perfectly concealed.

To analyze the security of the subliminal channel, we note that anyone who can recover k from public information and the signed message, (m;r,s) can almost certainly also recover the T_X's secret key x. To do this, he first hashes m to form h = H(m), and then if (r,p-1) = 1 so that r^{-1} exists, then x is easily found from;

$$x = r^{-1} (h-ks) \mod (p-1) \quad . \tag{1}$$

The probability that ($\alpha^k \bmod p$, p-1) = 1 given that (k,p-1) = 1, is asymptotically (with p) $\varphi(p-1)/(p-1)$, since this is the exact value for the probability when k is unrestricted, and the modular exponentiation operation behaves like a uniform random mapping onto the residues modulo p-1. In fact, the security of almost all public key cryptoschemes is dependent on this random mapping property of the modular exponentiation operator.

If (r,p-1) = f > 1 so that r does not have a multiplicative inverse, we can still solve for x in almost all cases using the forward search cryptoanalytic technique devised by Holdridge and Simmons [8] as a means to attack a public key secrecy channel in those cases in which the source equivocation is small enough to make an exhaustive search feasible. In such situations, even if the encryption operation is impossible to invert, since the encryption key is public it is feasible for the cryptanalyst to preencrypt plaintexts to generate a table of plaintext/ciphertext pairs, and then use table lookup to find the plaintext corresponding to a ciphertext—even though direct decryption is impossible. In the application being discussed here, inverting $y = \alpha^x$ to recover x directly is the hard problem of taking discrete logarithms (with respect to α). We can, however, in almost all instances, establish that x is an element in a set Z whose cardinality is small enough that it is feasible to calculate the modular exponentiation, α^{x_i}, for all $x_i \in Z$. It is then an easy matter to identify x itself.

To carry out a forward search for the user's secret key, x, when (r,p-1) > 1, we reduce (1)

$$z = \left(\frac{r}{f}\right)^{-1} \left(\frac{h-ks}{f}\right) \mod \left(\frac{p-1}{f}\right) \tag{2}$$