3. both Pícara and Vivales are certain that conditions (1) and (2) hold.

At first glance, this might seem like an odd thing to want. However, such a channel turns out to be a fundamental concept in cryptography. We shall soon see how it can be used to construct a non-interactive zero-knowledge proof. But before discussing this application to zero knowledge, we describe one way to obtain an oblivious transfer channel, based on the intractability of the discrete log problem.

More precisely, we suppose that we have a large finite field $\mathbf{F}_q$ and a fixed element b of the multiplicative group $\mathbf{F}_q^*$ such that, given b^x and b^y, there is no computationally feasible way to find b^{xy}. This is the Diffie–Hellman assumption, which conjecturally holds if the discrete logarithm problem is intractable in $\mathbf{F}_q^*$ (see §3).

We further suppose that we have an easily computed (and easily inverted) map ψ from our finite field to the $\mathbf{F}_2$-vector space $\mathbf{F}_2^n$ of n-tuples of bits. Suppose that the image of this map contains all of $\mathbf{F}_2^{n-1}$ (i.e., all n-tuples whose last bit is 0). For example, if q is a prime p, then we can choose n so that $2^{n-1} < p < 2^n$, and map any element of $\mathbf{F}_q$ — i.e., any nonnegative integer less than p — to its sequence of binary digits.

We suppose that our message units are also n-tuples of bits, i.e., elements $m \in \mathbf{F}_2^n$. We finally suppose that an element $C \in \mathbf{F}_q^*$, fixed once and for all, has been chosen so that no one knows its discrete logarithm. (Recall that we have assumed that the discrete log problem is intractable in $\mathbf{F}_q^*$.) This element C might have been supplied by a "trusted Center," or by an agreed upon random procedure, or by an interactive construction in which both Pícara and Vivales participated.

The oblivious transfer proceeds as follows. Vivales chooses a random integer x, $0 < x < q-1$, and also a random element $i \in \{1,2\}$. In what follows both x and i denote fixed integers in the range $\{1,\dots,q-2\}$ and $\{1,2\}$, respectively. Vivales sets $\beta_i = b^x$ and $\beta_{3-i} = C/b^x$. He then publishes his "public key" (β_1,β_2), while keeping x and i secret. Notice that Vivales is assumed not to know the discrete logarithm of β_{3-i} — which we shall denote x' — because if he did, then he would know the discrete log of $C = \beta_i\beta_{3-i}$, contrary to assumption.

Now suppose that Pícara has a message unit $m_1 \in \mathbf{F}_2^n$ from the first packet and a message unit $m_2 \in \mathbf{F}_2^n$ from the second packet. She chooses two random integers $0 < y_1, y_2 < q-1$, and sends to Vivales the following two elements of $\mathbf{F}_q^*$ and two elements of $\mathbf{F}_2^n$:

$$b^{y_1}, \qquad b^{y_2}; \qquad\qquad \alpha_1 = m_1 + \psi(\beta_1^{y_1}), \qquad \alpha_2 = m_2 + \psi(\beta_2^{y_2}).$$

(Here addition is in the $\mathbf{F}_2$-vector space $\mathbf{F}_2^n$; this addition operation is also known as "exclusive or.") Pícara keeps y_1 and y_2 secret.

Since $\beta_i^{y_i} = (b^{y_i})^x$, and Vivales knows both b^{y_i} and x, he can easily determine $\psi(\beta_i^{y_i})$, and hence find $m_i = \alpha_i + \psi(\beta_i^{y_i})$. However, if he wanted to find m_{3-i}, he would have to find $\beta_{3-i}^{y_{3-i}} = b^{x'y_{3-i}}$ knowing only $b^{y_{3-i}}$ and $b^{x'}$ but not y_{3-i} or x'. This is impossible, by the Diffie–Hellman assumption.