A.A. Let U be a 2×2 matrix whose first column is $|\omega\rangle$ and whose second column is a unit vector $|\chi\rangle$ such that $\langle\chi|\omega\rangle = 0$. For example, one could set

$$U = \begin{bmatrix} \omega_0 & -\overline{\omega_1} \\ \omega_1 & \overline{\omega_0} \end{bmatrix}.$$

Then U is unitary, and so is U^*, and hence U^* is a valid quantum gate. If Babatope's $|\beta\rangle = |0\rangle$, then he measures $|\psi\rangle$. If $|\beta\rangle = |1\rangle$, then he measures $U^*|\psi\rangle$. The rest of the protocol is unchanged.

[That's a sketch of an answer. I leave it to you to prove that U is unitary and to understand why this works. Certainly you should check that when $|\omega\rangle = |+\rangle$ we recover the original protocol.]

A.B. It's bad for Ariko and Babatope to use a $|\omega\rangle$ such that $\langle 0|\omega\rangle = 0$. For then the matrix

$$V = \begin{bmatrix} 1 & \omega_0 \\ 0 & \omega_1 \end{bmatrix},$$

which has $|0\rangle$ and $|\omega\rangle$ in its columns, is unitary, and Ariko's encoding of $|\alpha\rangle$ into $|\psi\rangle$ amounts to $|\psi\rangle = V|\alpha\rangle$. Einar, upon intercepting Ariko's $|\psi\rangle$, can measure $V^*|\psi\rangle$, recover $|\alpha\rangle$ with probability 1, reconstruct $|\psi\rangle = V|\alpha\rangle$, and pass this $|\psi\rangle$ on to Babatope without detection.

[This is a slightly easier version of a problem that appeared in our homework. By the way, the title of Bennett's 1992 paper was, "Quantum cryptography using any two nonorthogonal states". Beyond non-orthogonality, you probably want your two encoding vectors to be as far from parallel as possible and as far from orthogonal as possible, to improve the probabilities. That's why $|0\rangle$ and $|+\rangle$ are the standard.]

B. The state $|\psi\rangle$ can be written

$$\begin{aligned} |\psi\rangle &= \begin{bmatrix} \psi_{00} \\ \psi_{01} \\ \psi_{10} \\ \psi_{11} \end{bmatrix} \\ &= \sqrt{|\psi_{00}|^2 + |\psi_{10}|^2} \begin{bmatrix} \frac{\psi_{00}}{\sqrt{|\psi_{00}|^2+|\psi_{10}|^2}} \\ 0 \\ \frac{\psi_{10}}{\sqrt{|\psi_{00}|^2+|\psi_{10}|^2}} \\ 0 \end{bmatrix} + \sqrt{|\psi_{01}|^2 + |\psi_{11}|^2} \begin{bmatrix} 0 \\ \frac{\psi_{01}}{\sqrt{|\psi_{01}|^2+|\psi_{11}|^2}} \\ 0 \\ \frac{\psi_{11}}{\sqrt{|\psi_{01}|^2+|\psi_{11}|^2}} \end{bmatrix} \\ &= \sigma|\chi\rangle|0\rangle + \tau|\phi\rangle|1\rangle, \end{aligned}$$

where

$$\begin{aligned}
\sigma &= \sqrt{|\psi_{00}|^2 + |\psi_{10}|^2}, \\
|\chi\rangle &= \frac{1}{\sigma}\begin{bmatrix} \psi_{00} \\ \psi_{10} \end{bmatrix}, \\
\tau &= \sqrt{|\psi_{01}|^2 + |\psi_{11}|^2}, \\
|\phi\rangle &= \frac{1}{\tau}\begin{bmatrix} \psi_{01} \\ \psi_{11} \end{bmatrix}.
\end{aligned}$$

Partial measurement of the second qbit produces

$$|\psi\rangle \mapsto \begin{cases} |\chi\rangle|0\rangle & \text{with probability } |\sigma|^2, \\ |\phi\rangle|1\rangle & \text{with probability } |\tau|^2. \end{cases}$$

In summary, we observe $|1\rangle$ on the second qbit with probability $|\tau|^2 = |\psi_{01}|^2 + |\psi_{11}|^2$.

C. We compute

$$\begin{aligned}
(H \otimes H) \cdot |1\rangle|0\rangle &= \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \\
&= \frac{1}{2}|0\rangle|0\rangle + \frac{1}{2}|0\rangle|1\rangle - \frac{1}{2}|1\rangle|0\rangle - \frac{1}{2}|1\rangle|1\rangle.
\end{aligned}$$

Then, by linearity, applying F yields

$$\begin{aligned}
& \frac{1}{2}|0\rangle|f(0)\rangle + \frac{1}{2}|0\rangle|1 \oplus f(0)\rangle - \frac{1}{2}|1\rangle|f(1)\rangle - \frac{1}{2}|1\rangle|1 \oplus f(1)\rangle \\
=\ & \frac{1}{2}|0\rangle|0\rangle + \frac{1}{2}|0\rangle|1\rangle - \frac{1}{2}|1\rangle|0\rangle - \frac{1}{2}|1\rangle|1\rangle \\
=\ & \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
=\ & |-\rangle|+\rangle
\end{aligned}$$

no matter what $f(0)$ and $f(1)$ are. The Hadamard layer transforms this state to $|1\rangle|0\rangle$. Thus measurement of the first qbit produces $|1\rangle$ with probability 1, no matter what the details of f are. In summary, this version of the algorithm is useless.

D. We have proved in homework that $(U \otimes V)^* = U^* \otimes V^*$. Then, using the fact that $(A \otimes C)(B \otimes D) = AB \otimes CD$, we have

$$\begin{aligned}
(U \otimes V)^*(U \otimes V) &= (U^* \otimes V^*)(U \otimes V) \\
&= U^*U \otimes V^*V \\
&= I \otimes I \\
&= I.
\end{aligned}$$

Thus $U \otimes V$ is unitary.