em nenhum dos passos ela utiliza de outras informações para responder Beto e, no fim dos passos, Beto saberá, com grande probabilidade, que Alice conhece o valor de S.

4. Como descrito, todas as pessoas, por exemplo, Beto, recebem diretamente de T os valores p, q, b.

5 Beto pode solicitar que T assine (I_A, V) de Alice e comparar com o valor do certificado da (chave pública) da 1ª etapa do protocolo de identificação.

6. Temos:

$z = b^y v^e \bmod p$

$z = b^{se} . b^r . v^e \bmod p$

$z = (b^s . v)^e . b^r \bmod p$

$z = (b^s . b^{-s})^e . b^r \bmod p$

$z = b^r \bmod p = x$

7. Como visto em (2), Carlos não pode descobrir os parâmetros privados de Alice. Ele pode, porém, chutar um valor de e no passo (1) e, com um y qualquer, enviar $x = b^y v^e \bmod p$ no passo 1 e enviar y no passo 3. Concluo, a probabilidade de acertar o valor de e é $1/2^t$.

4. Após concluir a comunicação com Alice, se $z = x$, então b, p, q de Alice são os certos, pois, Beto usa o b e o p de T em seus cálculos e o resultado foi o mesmo do informado por Alice na 1ª etapa: $x = b_{ALICE}^{r} \bmod p_{ALICE}$