Protocols Championship Submission

[redacted]

[redacted]

Description of the Protocol

The protocol can be described as follows:

$$A \to S : \{\{n\}_{pub(B)}\}_{k(A,S)}$$
$$S \to B : A, \{n\}_{pub(B)}$$
$$B \to A : h(n)$$
$$A \to B : h(B, n)$$

Initial knowledge: We suppose that agents A, B and S initially know public keys $pub(C)$ of agent C, for any agent C. A and B also share symmetric keys $k(A, S)$ and $k(B, S)$ respectively with the server S.

Data generated during the protocol: A generates a nonce n, which is to be shared secretly with B.

Protocol Description: Alice starts the protocol by asymmetrically encrypting a freshly generated nonce n with Bob's public key (we assume that only Bob has access to the corresponding secret key $priv(B)$), and then symmetrically encrypting this term with her shared key with the server. She then sends this term to the server.
The server symmetrically decrypts this message with her shared key with Alice. She then pairs the decrypted message with Alice's identity, and sends it to Bob.
Bob decrypts the second part of this message asymmetrically with $priv(B)$) to access the identity-nonce pair inside. He now responds to Alice, by sending her a hash of the nonce.
Alice checks the hash of her original nonce, and if it matches the message she has received from Bob, she sends him a hash of the pair (B, n). Bob checks to see if the message he received from Alice is indeed a hash of the pair formed by concatenating his identity with the nonce he has, and if it is, the protocol is successfully completed.
Cost of protocol = 131

Security properties

- Authentication: When Bob receives $h(B, n)$, this message was sent by Alice.
- Confidentiality: Both Alice and Bob are the only ones to know n.