Security Protocols and Verification

Defense of Cryptographic Protocol

Garance Frolla
Ely Marthouret
Ewan Decima

Team: **ASKO OM8464A2**

September / November 2025

Contents

1 Attack from BitSentinel **2**
1.1 The attack 2
1.2 Refutation 2

2 Conclusion **2**

1 Attack from BitSentinels

1.1 The attack

You will find below a concise summary of your attack against our protocol.

1. $I \to B : \{|\langle A, N_I \rangle|\}_{K'}$
2. $I \to S : \{|\langle B, \tau, \lambda, K' \rangle|\}_{K_{IS}}$
3. $S \to B : \{|\langle A, \tau, \lambda, K' \rangle|\}_{K_{BS}}$
4. $B \to I(A) : \{|N_I + 1|\}_{K'}$

1.2 Refutation

Your attack is based on two assumptions of yours:

- In the second message I does not communicate his interlocutor, but he does.
- S does not know who sent the second message, but in fact he does: he just used K_{IS} to decipher the second message, so S knows that the sender of the second message is I, not A. So the third message, sent by S should be

$$S \to B : \{|\langle I, \tau, \lambda, K' \rangle|\}_{K_{BS}}$$

So B will know that the message is coming from I and not A. In fact, B will decipher the first message and will spot the difference between the identity contained in the first message and the identity of the sender contained in the third message ($I \neq A$).

2 Conclusion

We refuse this attack, but we are ready to face another one.