Paper title and authors; where appeared.

Dolev and Yao, *On the Security of Public Key Protocols.* IEEE Trans. Inf. Theory, 1983.

What is the main problem this paper attacks?

Suppose that we are given a "ping-pong" protocol in which two participants send messages back and forth, at each step applying a particular sequence of operators, including public key encryption and decryption. How can we decide whether the adversary can manipulate the regular participants into disclosing a message M, which is supposed to remain secret?

What solution does the paper propose?

The authors show that for simple protocols ("cascade" protocols), a very simple balance property is enough. For protocols that can add name stamps, and check whether an incoming message has the right name, they give a much more complicated algorithm.

What central idea did the authors use to solve it?

They regard E_x and D_x as symbolic operators which cancel. They then solve the problems by analyzing string concatenations.

What is a weakness or limitation of the paper?

The protocols in this paper never contain nonces, which makes the analysis problem far more complex, indeed undecidable in general.

Why is this paper important?

This paper introduced the idea of treating the cryptographic operators are purely symbolic operators with cancellation (rewriting) rules. It also made clear that the strong Needham-Schroeder adversary model fits very nicely with symbolic analysis.