Flaw in NTRU Signature Scheme (NSS)

In a presentation at Eurocrypt 2001 on Tuesday, May 8 in Innsbruck, Austria, RSA Laboratories scientists Jakob Jonsson and Michael Szydlo indicated they have found a flaw in an initial version of the NTRU Signature Scheme (NSS), leading to two different types of practical attacks.

The first attack enables an opponent, given a modest number of signatures (say, 100,000) generated with a private signature key, to determine the signature key and thereby forge an unlimited number of new signatures.

The second attack enables an opponent, given only the signer's public key and no signatures at all, to forge an unlimited number of new signatures.

The attacks were discovered at RSA Laboratories in late March and subsequently communicated to NTRU's scientists. Independently, Jacques Stern (ENS) and Craig Gentry (DoCoMo Communications Laboratories) also developed attacks similar to the second attack. RSA Laboratories is currently evaluating whether the attacks can be extended to the recently enhanced version of NSS.

A summary of RSA Laboratories' results is found in the presentation given at Eurocrypt.