Compromising DSA and ElGamal Signatures

Jonathan Hammell
Computer Science, University of Calgary
jhammell@cpsc.ucalgary.ca

Abstract

"Kleptography" is a name given to a type of attack that uses malicious code to leak secret information that could thwart cryptographic systems in an undetectable way. Kleptography had its beginnings in the subliminal channels of Simmons. This talk will be a survey of research in subliminal channels and kleptographic attacks against the ElGamal signature scheme and its variant, the U.S. Digital Signature Algorithm (DSA).