1035-11-1146 **Ning Shang*** (nshang@math.purdue.edu), 150 N. University Street, West Lafayette, IN 47907, **Elisa Bertino** (bertino@cs.purdue.edu), Purdue University, Department of Computer Science, 305 N. University Street, West Lafayette, IN 47907, and **Samuel S. Wagstaff** (ssw@cerias.purdue.edu), Purdue University, Department of Computer Science, 305 N. University Street, West Lafayette, IN 47907. *An Efficient Time-Bound Hierarchical Key Management Scheme for Secure Broadcasting.*

In electronic subscription and pay TV systems, data can be organized and encrypted using symmetric key algorithms according to predefined time periods and user privileges, then broadcast to users. This requires an efficient way to manage the encryption keys. In this scenario, time-bound key management schemes for a hierarchy were proposed by Tzeng and Chien in 2002 and 2005, respectively. Both schemes are insecure against collusion attacks. We propose a new key assignment scheme for access control which deploys elliptic curve cryptography. This scheme is both efficient and secure. We also provide analysis of the scheme with respect to security and efficiency issues. (Received September 18, 2007)