

998-68-34

**Jessica N Staddon\*** (staddon@parc.com), 3333 Coyote Hill Road, Palo Alto, CA 94304.

*Inference Control*. Preliminary report.

Some database queries are clearly not privacy-preserving; for example, queries that return social security numbers. Other queries may at first glance appear to be privacy-preserving, although they actually leak personal information through *inference*. To see this, note that queries that return zip code or car make or city of residence may each be innocuous when made individually, but when made together, the information that's returned may suffice to identify an individual. Many techniques have been developed for identifying such inference channels in large databases. The subject of this talk is cryptographic techniques for ensuring no undesired inferences can be made once the inference channels have been identified. We discuss combinatorial access control techniques that provide inference control with flexible information access and fast query response. We also discuss how to ensure *private* inference control; that is, protection against inferences when the database server doesn't know what queries are being made.

Some of this talk covers joint work with David Woodruff. (Received January 03, 2004)