# THE DINING CRYPTOGRAPHERS IN THE DISCO:

## *UNCONDITIONAL SENDER AND RECIPIENT UNTRACEABILITY WITH COMPUTATIONALLY SECURE SERVICEABILITY*

Michael Waidner Birgit Pfitzmann

Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe
Postfach 6980, D-7500 Karlsruhe 1, F.R. Germany

**Abstract**

In Journal of Cryptology 1/1 (1988) 65–75, CHAUM describes a beautiful technique, the *DC-net*, which should allow participants to send and receive messages anonymously in an arbitrary network. The untraceability of the senders is proved to be unconditional, but that of the recipients implicitly assumes a *reliable* broadcast network. This assumption is unrealistic in some networks, but it can be removed completely by using the fail-stop key generation schemes by WAIDNER (these proceedings). In both cases, however, each participant can untraceably and permanently disrupt the entire DC-net.

We present a protocol which guarantees *unconditional untraceability*, the original goal of the DC-net, on the *inseparability assumption* (i.e. the attacker must be unable to prevent honest participants from communicating, which is considerably less than reliable broadcast), and *computationally secure serviceability*: Computationally restricted disrupters can be identified and removed from the DC-net.

On the one hand, our solution is based on the lovely idea by CHAUM of setting traps for disrupters. He suggests a scheme to guarantee unconditional untraceability and computationally secure serviceability, too, but on the reliable broadcast assumption. The same scheme seems to be used by BOS and DEN BOER (these proceedings). We show that this scheme needs some changes and refinements before being secure, even on the reliable broadcast assumption.

On the other hand, our solution is based on the idea of *digital signatures whose forgery by an unexpectedly powerful attacker is provable*, which might be of independent interest. We propose such a (one-time) signature scheme based on claw-free permutation pairs; the forgery of signatures is equivalent to finding claws, thus in a special case to the factoring problem. In particular, with such signatures we can, for the first time, realize *fail-stop Byzantine Agreement*, and also *adaptive Byzantine Agreement*, i.e. Byzantine Agreement which can only be disrupted by an attacker who controls at least a third of all participants *and* who can forge signatures.

We also sketch applications of these signatures to a payment system, solving disputes about shared secrets, and signatures which cannot be shown round.

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, p. 690, 1990.