Justification for *Broadcast Encryption with Free-Riders and Unconditional Security*

Andre Adelsbach and Ulrich Greveler

Horst Görtz Institute for IT Security
Ruhr University Bochum
Germany
(andre.adelsbach,ulrich.greveler)@nds.rub.de

Solutions to the problem of transmitting data to a group of receivers in a way that only the privileged subset of all possible receivers can decrypt the data is needed by a number of applications: pay-TV, audio streaming, real-time business data are popular applications.

In our submission we present two schemes for efficient broadcast key establishment that enables a sender to communicate to any subset of the user-base by allowing a small ratio of *free-riders*. The schemes do not require stateful receivers and one scheme is unconditionally secure.

There are a number of proposed methods to construct a broadcast encryption scheme with different properties since Fiat and Naor introduced the concept in 1993 and it was shown that certain lower bounds regarding the size of the message header or user key space can not be exceeded.

The security paradigm shift we propose here is to relax the requirement and solve the problem of secure broadcast communication by a probabilistic approach. The relaxed condition we consider is that not only the privileged users (e.g., who paid for a pay-tv transmission) can decrypt the message but also a small number of free-riders can do so **as long as these free-riders cannot anticipate their status for the next upcoming transmission and make their payment decision dependant on that**. Accepting this relaxation we can enhance efficiency and – particularly with regard to message header lenght – there is no need to address all privileged users individually as it is often done in current pay-tv implementations.

Thus we present a new severalfold trade-off facet for broadcast encryption with specified relaxed requirements, namely the number (or ratio) of free-riders vs. the number of messages to be sent and the number of keys stored by each user. This new approach to an old problem may foster further advance in broadcast encryption.

Attendance Statement as required by the CfP: One author wishes to attend the workshop.