Low Overhead Broadcast Encryption from Multilinear Maps

Abstract

We use multilinear maps to provide a solution to the long-standing problem of public-key

broadcast encryption where all parameters in the system are small. In our constructions,

ciphertext overhead, private key size, and public key size are all poly-logarithmic in the total

number of users. The systems are fully collusion-resistant against any number of colluders. All

our systems are based on an O(log N )-way multilinear map to support a broadcast system for N

users. We present three constructions based on different types of multilinear maps and providing

different security guarantees. Our systems naturally give identity-based broadcast systems with

short parameters.

1

Introduction

Broadcast encryption [FN94] is an important generalization of public-key encryption to the multi-

user setting. In a broadcast encryption scheme, a broadcaster encrypts a message for a subset S of

users who are listening on a broadcast channel. The broadcaster can encrypt to any set S of its

choice, and any user in S can decrypt the broadcast using its secret key. The system is said to be

fully collusion resistant if even a coalition of all users outside of S learns nothing about the plaintext.

Broadcast systems are regularly used in TV and radio subscription services where broadcasts are

encrypted for currently active subscribers. They are also used in encrypted file systems where a file

is encrypted so that only users who have access to the file can decrypt it.

The efficiency of a broadcast system is measured in the ciphertext overhead: the number of bits

in the ciphertext beyond what is needed for the description of the recipient set S and the symmetric

encryption of the plaintext payload. The shorter the overhead, the better. We say that the system

has low overhead if the ciphertext overhead depends at most logarithmically on the number of

users N in the system.

Existing constructions with low ciphertext overhead. Several broadcast systems are fully

collusion resistant with low ciphertext overhead. The first such system by Boneh, Gentry, and

Waters [BGW05] is built from bilinear maps. It has constant ciphertext overhead and short secret

keys, but the public encryption key size is linear in the number of users N . Other systems using

bilinear-maps achieve adaptive security [GW09, DPP07] and some are even identity-based [GW09,

Del07, SF07], but the public encryption key is always large.

Multilinear maps give secret-key broadcast systems with optimal ciphertext overhead [BS03,

GGH13a, FHPS13, CLT13, BW13]. However, in these systems the broadcaster’s key must be kept

secret, and they require an N -way multilinear map to support N users. Current constructions

of N -linear maps [GGH13a, CLT13] have group elements of size O(N 2 ) bits, resulting in large

space requirements. While these broadcast systems can be made public-key by including a few

group elements in the ciphertext, their dependence on N -linear maps leads to an O(N 2 ) ciphertext

overhead, which is worse than the trivial broadcast system. Until this work, it has not been known

how to use multilinear maps to construct low overhead broadcast systems with a short public

encryption key.

A third class of constructions employs the powerful candidates for indistinguishability obfus-

cation (iO) [BGI + 01, GGH + 13b]. Using iO it is possible to build a public-key broadcast system

with optimal ciphertext overhead and short private keys, though public keys are large [BZ13]. The

resulting systems have several other remarkable properties. However, current iO candidates add

considerable complexity on top of multilinear maps. Our goal here is to construct broadcast systems

using only simple assumptions on multilinear maps, namely, without relying on iO.

Our results. We describe three broadcast systems for N users that use an O(log N )-way multi-

linear map. The systems have ciphertext overhead and decryption key of only O(1) group elements

which is O(log 2 N ) bits using the current multilinear map candidates. The public encryption key

contains O(log N ) group elements which is O(log 3 N ) bits. The first system uses an asymmetric

multilinear map and follows the [BGW05] construction closely. It uses the O(log N )-way multilinear

map to compress the public key of that system from O(N ) group elements to O(log N ) elements

while keeping the ciphertext overhead and secret key short. We prove static security under a

multivariate equivalent of the [BGW05] assumption.

The second system uses a general symmetric O(log N )-way multilinear map to similarly compress

the public key in [BGW05]. The added flexibility of a symmetric map has both positive and

negative consequences. On the negative side, this flexibility allows the adversary to combine extra

elements together. To maintain security we must ensure that all user indexes u ∈ [N ] are mapped to

integers û ∈ [O(N log N )] where all û have the same Hamming weight. This mapping does not affect

ciphertext or private key size. On the positive side, this flexibility allows us to obtain slightly better

parameters and base static security on a slightly simpler, though similar, complexity assumption.

The third system is built from a symmetric O(log N )-way map, but we can prove adaptive

security of the scheme in generic multilinear groups. This system has secret keys of length O(log 3 N )

bits, which is longer than the previous two schemes, but has a tighter security proof in generic

groups.

Because the parameters of these systems are logarithmic in N , we can let N be exponential,

and in particular be as large as the range of a collision resistant hash function (e.g., N = 2 256 ).

This, in effect, turns all our broadcast systems into efficient identity-based schemes. A user with

identity id ∈ {0, 1} ∗ is given the secret key associated with index number H(id) ∈ [N ] where H is a

collision resistant hash whose range is [N ]. A broadcaster can then transmit to a set of recipients

simply by hashing their public identities. For this reason, we describe all our broadcast systems as

identity-based broadcast schemes.

Additional related work. Collusion resistant broadcast encryption has been widely studied.

Revocation systems (e.g., [NNL01, HS02, GST04, DF02, LSW10]) can encrypt to N − r users with ciphertext size of O(r). Further combinatorial solutions (e.g., [NP00, DF03]) achieve similar

parameters. A broadcast encryption system is said to be recipient-private if broadcast ciphertexts

reveal nothing about the intended set of recipients [BBW06, LPQ12, FP12]. Our broadcast

systems are not recipient private, and it is a long-standing open problem to build a low-overhead

recipient-private broadcast system. Such a system was recently built using indistinguishability

obfuscation [BZ13], but constructing such systems under weaker assumptions remains open.