# *Ad Hoc* Broadcast Encryption

Qianhong Wu
Dept. of Comp. Eng. and Maths
Universitat Rovira i Virgili, Tarragona, Catalonia
Key Lab. of AISTC,Ministry of Education
School of Computer, Wuhan University, China
qianhong.wu@urv.cat

Bo Qin
Dept. of Comp. Eng. and Maths
Universitat Rovira i Virgili, Tarragona, Catalonia
Dept. of Maths, School of Science
Xi'an University of Technology, China
bo.qin@urv.cat

Lei Zhang
Dept. of Comp. Eng. and Maths
Universitat Rovira i Virgili,Tarragona, Catalonia
lei.zhang@urv.cat

Josep Domingo-Ferrer
Dept. of Comp. Eng. and Maths
Universitat Rovira i Virgili, Tarragona, Catalonia
josep.domingo@urv.cat

## ABSTRACT

Numerous applications in *ad hoc* networks, peer-to-peer networks, and on-the-fly data sharing call for confidential broadcast without relying on a dealer. To cater for such applications, we propose a new primitive referred to as *ad hoc* broadcast encryption (AHBE), in which each user possesses a public key and, upon seeing the public keys of the users, a sender can securely broadcast to any subset of them, so that only the intended users can decrypt. We implement a concrete AHBE scheme proven secure under the decision Bilinear Diffie-Hellman Exponentiation (BDHE) assumption. The resulting scheme has sub-linear complexity, comparable to up-to-date broadcast systems which have also sub-linear complexity but require a fully trusted dealer.

## Categories and Subject Descriptors

E.3 [**Data Encryption**]: Public Key Cryptosystems

## General Terms

Security, Algorithm

## Keywords

Broadcast Encryption, Asymmetric Group Key Agreement, Ad Hoc Broadcast

## 1. INTRODUCTION

Broadcasting is one of the most useful, versatile, and well-studied communication primitives in distributed computing, with many applications. Existing broadcast encryption (BE) systems require a trusted dealer to produce and distribute secret keys to each user. Such systems provide efficient solutions to applications such as pay-TV and priced video distribution. Recently, efficient broadcast systems have been realized from bilinear pairings. Up-to-date BE schemes [2] enjoy adaptive security and sub-linear complexity with the scale of broadcast in terms of public key, decryption key (per user) and ciphertext.

Existing BE systems are not suitable for applications where the trusted dealer is unavailable. For instance, in *ad hoc*/peer-to-peer networks emerging in recent years, it is difficult to find an entity who can play the role of a trusted dealer to deploy a BE system. As another example, let us consider the following scenario in the traditional Internet. A company provides remote data storage services to registered users; users wish to be able to share their private files with some other registered users but do not want the company to see the contents of the shared files. In both scenarios, it is needed to build BE systems without requiring a trusted dealer. To meet this end, Wu *et al.* introduced the notion of asymmetric group key agreement [3] in which a public encryption key is negotiated. However, the protocol can only deal with the static case where the group of receivers cannot be chosen by the sender. Indeed, it is left open in that work [3] to construct a protocol allowing the sender to dynamically broadcast to any subset of potential receivers.

In this paper we close the gap left in Wu *et al.*'s work [3] by proposing a new primitive referred to as *ad hoc* broadcast encryption (AHBE). In an AHBE system, each user has a public/private key pair; knowing the public keys of the users, a sender can choose any subset of the users to broadcast; only the users in the receiver set can decrypt. We define an adaptive security notion in AHBE systems where the attacker adaptively corrupts users before choosing the receiver set to attack. It is easy to see that any regular public key encryption system implies an AHBE system in which, for $n$ receivers, $O(n)$ encryption operations and $O(n)$ ciphertexts are required. *The challenge is to design AHBE systems with short ciphertexts and efficient encryption.*

We address this challenge by presenting an AHBE scheme with short ciphertexts. The scheme is proven to be secure in the standard model under the decision BDHE assumption. The basic scheme has $O(n^2)$-size public key per user. Observing this shortcoming, we provide a tradeoff between ciphertexts and public keys. The resulting AHBE enjoys sub-linear complexity $O(n^{2/3})$ regarding both public keys and ciphertexts and $O(n^{1/3})$ regarding private keys. Our result is comparable to up-to-date regular broadcast systems, in which each receiver has also sub-linear complexity (*i.e.*, $O(\sqrt{n})$) regarding public/private keys and/or ciphertexts but require a fully trusted dealer.

*CCS'10,* October 4–8, 2010, Chicago, Illinois, USA.
ACM 978-1-4503-0244-9/10/10.

# 2. MODELING AHBE

For clarity, we define AHBE as a key encapsulation mechanism. An AHBE system consists of the following probabilistic algorithms.

**KeyGen**$(i, n, N)$**.** Let $N$ be the number of potential receivers, and $n \leq N$ be the maximal size of an AHBE recipient group. A user takes as input the system parameters $n, N$ and her index $i \in \{1, \cdots, N\}$, and outputs $\langle pk_i, sk_i \rangle$ as her public/secret key pair. Denote $\{\langle pk_i, sk_i \rangle | i \in \mathbb{R} \subseteq \{1, \cdots, N\}\}$ by $\langle pk_i, sk_i \rangle_{\mathbb{R}}$ and similarly, $\{\langle pk_i \rangle | i \in \mathbb{R} \subseteq \{1, \cdots, N\}\}$ by $\langle pk_i \rangle_{\mathbb{R}}$. Here, we leave the input security parameter $\lambda$, implicitly.

**AHBEnc**$(\mathbb{R}, \langle pk_i \rangle_{\mathbb{R}})$**.** This is the AHBE encryption algorithm. It is run by any sender who may or may not be in $\{1, \cdots, N\}$, provided that the sender knows the public keys of the potential receivers. It takes as input a recipient set $\mathbb{R} \subseteq \{1, \cdots, N\}$ and the public key $pk_i$ for $i \in \mathbb{R}$. If $|\mathbb{R}| \leq n$, it outputs a pair $\langle Hdr, \xi \rangle$ where $Hdr$ is called the header and $\xi$ is the secret session key in the key space $\mathbb{K}$. Send $(Hdr, \mathbb{R})$ to receivers.

**AHBDec**$(\mathbb{R}, j, sk_j, Hdr, \langle pk_i \rangle_{\mathbb{R}})$**.** This algorithm allows each receiver to decrypt the message encryption key $\xi$ hidden in the header. It takes as input the receiver set $\mathbb{R}$, an index $j \in \{1, \cdots, N\}$, the receiver's secret key $sk_j$, a header $Hdr$, the public/private key pairs of receivers in the recipient set $\mathbb{R}$. If $|\mathbb{R}| \leq n$, $j \in \mathbb{R}$, then the algorithm outputs the secret session key $\xi$.

## 2.1 Security Definitions

The correctness of an AHBE scheme is defined in the expected way, that is, any user in the receiver set can decrypt a valid header. As to security, we only define adaptive security against chosen plaintext attacks. However, our definition can readily be extended to capture chosen ciphertext attacks. Adaptive security in AHBE is defined using the following game between an attacker $\mathcal{A}$ and a challenger $\mathcal{CH}$. Both $\mathcal{CH}$ and $\mathcal{A}$ are given $\lambda$ as input.

**Setup.** The challenger runs $\mathsf{KeyGen}(i, n, N)$ to obtain the users' public keys. The challenger gives the public keys and public system parameters to the attacker.

**Corruption.** Attacker $\mathcal{A}$ adaptively issues private key queries for some indices $i \in \{1, \cdots, N\}$.

**Challenge.** At some point, the attacker specifies a challenge set $\mathbb{R}^*$, such that for the private key of any user $i$ queried in the corruption step we have that $i \notin \mathbb{R}^*$. The challenger sets $\langle Hdr^*, \xi_0 \rangle \leftarrow \mathsf{AHBEnc}(\mathbb{R}^*, \langle pk_i \rangle_{\mathbb{R}^*})$ and $\xi_1 \leftarrow \mathbb{K}$. It sets $b \leftarrow \{0, 1\}$ and gives $(Hdr^*, \xi_b)$ to attacker $\mathcal{A}$.

**Guess.** Attacker $\mathcal{A}$ outputs a guess bit $b' \in \{0, 1\}$ for $b$ and wins the game if $b = b'$.

*Definition 1.* **(Adaptive security.)** We define $\mathcal{A}$'s advantage in attacking the AHBE system with security parameter $\lambda$ as $Adv^{\texttt{AHBE}}_{\mathcal{A},n,N}(1^\lambda) = |\Pr[b = b'] - \frac{1}{2}|$. We say that an AHBE scheme is adaptively secure if for all polynomial time algorithms $\mathcal{A}$ we have that $\mathrm{Adv}^{\texttt{AHBE}}_{\mathcal{A},n,N}(1^\lambda)$ is negligible in $\lambda$.

In addition to the adaptive game for AHBE security, we consider a weaker security notion referred to as *semi-static* security. In this game the adversary must commit to a set $\tilde{\mathbb{R}}$ of indices at the $\mathsf{Initialization}$ phase before the $\mathsf{Setup}$ stage. The adversary cannot query the private key for any $i \in \tilde{\mathbb{R}}$, and it must choose a target group $\tilde{\mathbb{R}}^*$ for the challenge ciphertext that is a subset of $\tilde{\mathbb{R}}$. A semi-static adversary is weaker than an adaptive adversary, but it is stronger than a static adversary who has to commit to its target group $\tilde{\mathbb{R}}^*$ for the challenge ciphertext at the $\mathsf{Initialization}$ phase, since the semi-static attacker's choice of which subset of $\tilde{\mathbb{R}}$ to attack can be adaptive.

## 2.2 From Semi-static Security to Adaptive Security

In the sequel we show how to convert an AHBE system with semi-static security into one with adaptive security. The cost is doubling public keys and ciphertexts. Let $\mathcal{E}_{sym}$ be a symmetric encryption scheme with key space $\mathbb{K}$, and $E(\cdot)$ and $D(\cdot)$ be the encryption and decryption algorithms, respectively. Suppose we are given a semi-static secure AHBE system $\texttt{AHBE}_{SS}$ with algorithms $KeyGen_{SS}$, $AHBEnc_{SS}$, $AHBDec_{SS}$. Then we can build an adaptively secure $\texttt{AHBE}_A$ system as follows.

**KeyGen.** A user generates a public/secret key pair by doing: $s_i \leftarrow \{0, 1\}$, $(pk'_{2i-1}, sk'_{2i-1}) \leftarrow KeyGen_{SS}(2i-1, 2n, N)$, $(pk'_{2i}, sk'_{2i}) \leftarrow KeyGen_{SS}(2i, 2n, N)$. Set $pk_i = (pk'_{2i-1}, pk'_{2i})$, $sk_i = (sk'_{2i-s_i}, s_i)$. Output $(pk_i, sk_i)$.

**AHBEnc.** For a session key $\zeta$ to be broadcast, the sender does the following. Generate a random set of $|\mathbb{R}|$ bits: $t \leftarrow \{t_i \leftarrow \{0, 1\} : i \in \mathbb{R}\}$. Set $\mathbb{R}_0 = \{2i - t_i : i \in \mathbb{R}\}$, $\langle Hdr_0, \xi_0 \rangle = AHBEnc_{SS}(\mathbb{R}_0, \langle pk'_\ell \rangle_{\mathbb{R}_0})$, $\mathbb{R}_1 = \{2i - (1 - t_i) : i \in \mathbb{R}\}$, $\langle Hdr_1, \xi_1 \rangle = ABHEnc_{SS}(\mathbb{R}_1, \langle pk'_\ell \rangle_{\mathbb{R}_1})$, $C_0 = E(\zeta, \xi_0)$, $C_1 = E(\zeta, \xi_1)$, $Hdr = \langle Hdr_0, C_0, Hdr_1,\ C_1, t \rangle$. Output $\langle Hdr, \zeta \rangle$. Send $(Hdr, \mathbb{R})$ to receivers.

**AHBDec.** Receiving $(Hdr, \mathbb{R})$, a user in $\mathbb{R}$ does the following. Parse $sk_j$ as $\langle sk'_j, s_j \rangle$, Parse $Hdr$ as $\langle Hdr_0, C_0, Hdr_1, C_1, t \rangle$. Set $\mathbb{R}_0$ and $\mathbb{R}_1$ as above. Compute
$\xi_{s_j \oplus t_j} \leftarrow AHBDec_{SS}(\mathbb{R}_{s_j \oplus t_j}, j, sk'_j, Hdr_{s_j \oplus t_j}, \langle pk'_\ell \rangle_{\mathbb{R}_{s_j \oplus t_j}})$,
$\zeta = D(C_{s_j \oplus t_j}, \xi_{s_j \oplus t_j})$. Output $\zeta$.

As to the security of the transformation, we have the following theorem whose proof can be found in the full version of the paper.

Theorem 1. *Let $\mathcal{A}$ be an adaptive attacker against $\texttt{AHBE}_A$. Then, there exist algorithms $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$, and $\mathcal{B}_4$, each running in about the same time as $\mathcal{A}$, such that $Adv^{\texttt{AHBE}_A}_{\mathcal{A},n,N}(\lambda) \leq Adv^{\texttt{AHBE}_{SS}}_{\mathcal{B}_1,2n,N}(\lambda) + Adv^{\texttt{AHBE}_A}_{\mathcal{B}_2,2n,N}(\lambda) + Adv^{\mathcal{E}_{sym}}_{\mathcal{B}_3}(\lambda) + Adv^{\mathcal{E}_{sym}}_{\mathcal{B}_4}(\lambda)$.*

# 3. THE PROPOSALS

The scheme is realized in bilinear pairing groups and its security relies on the decision $n$-BDHE assumption, which is shown to be sound by Boneh *et al.* [1]. Let $\texttt{PairGen}$ be an algorithm that, on input a security parameter $1^\lambda$, outputs a tuple $\Upsilon = (p, \mathbb{G}, \mathbb{G}_T, e)$, where $\mathbb{G}$ and $\mathbb{G}_T$ have the same prime order $p$, and $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is an efficient non-degenerate bilinear map such that $e(g, g) \neq 1$ for any generator $g$ of $\mathbb{G}$, and for all $u, v \in \mathbb{Z}$, it holds that $e(g^u, g^v) = e(g, g)^{uv}$.

### 3.1 AHBE with Small Ciphertexts

Let $h_1, \cdots, h_n$ be independent generators of $\mathbb{G}$. In what follows we implement an AHBE scheme with short ciphertexts by exploiting bilinear pairings.

- **KeyGen.** For $i \in \{1, \cdots, N\}$, user $i$ randomly chooses $x_{i,1}, \cdots, x_{i,n}$, $r_{i,1}$, $\cdots$, $r_{i,n} \in \mathbb{Z}_p$ and computes
$$\langle X_{i,1}, \cdots, X_{i,n}\rangle = \langle e(g,g)^{x_{i,1}}, \cdots, e(g,g)^{x_{i,n}}\rangle$$
$$\langle R_{i,1}, \cdots, R_{i,n}\rangle = \langle g^{r_{i,1}}, \cdots, g^{r_{i,n}}\rangle.$$
For $k = 1, \cdots, n$, user $i$ computes
$$s_{i,k} = \langle s_{i,k,1}, \cdots, s_{i,k,k-1}, s_{i,k,k+1}, \cdots, s_{i,k,n}\rangle$$
$$= \langle g^{x_{i,k}} h_1^{r_{i,k}}, \cdots, g^{x_{i,k}} h_{k-1}^{r_{i,k}}, g^{x_{i,k}} h_{k+1}^{r_{i,k}}, \cdots, g^{x_{i,k}} h_n^{r_{i,k}}\rangle.$$
Output user $i$'s public key
$$PK_i = \{s_{i,k}\}_{1 \le k \le n} \cup \{X_{i,1}, \cdots, X_{i,n}, R_{i,1}, \cdots, R_{i,n}\}.$$
Output user $i$'s secret key
$$s_i = \langle x_{i,1}, \cdots, x_{i,n}, r_{i,1}, \cdots, r_{i,n}\rangle.$$

- **AHBEnc.** The sender selects a receiver set $\mathbb{R} = \{i_1, \cdots, i_t\} \subseteq \{1, \cdots, N\} (t \le n)$. The sender computes
$$R = \prod_{j=1}^{t} R_{i_j,j} \prod_{j=t+1}^{n} R_{i_t,j}$$
$$= g^{\sum_{j=1}^{t} r_{i_j,j} + \sum_{j=t+1}^{n} r_{i_t,j}} \overset{\texttt{Def}}{=} g^r,$$
$$X = \prod_{j=1}^{t} X_{i_j,j} \prod_{j=t+1}^{n} X_{i_t,j}$$
$$= e(g,g)^{\sum_{j=1}^{t} x_{i_j,j} + \sum_{j=t+1}^{n} x_{i_t,j}} \overset{\texttt{Def}}{=} e(g,g)^x.$$
The sender sets the broadcast public key as $PK = (R, X)$ for receivers $\mathbb{R}$. The sender computes the header $Hdr = (c_1, c_2)$ :
$$\gamma \overset{R}{\leftarrow} \mathbb{Z}_p, c_1 = g^\gamma, c_2 = R^{-\gamma}.$$
Set $\xi = X^\gamma$ and output $\langle Hdr, \xi\rangle$. Send $\langle \mathbb{R}, Hdr\rangle$ to receivers.

- **AHBDec.** Each receiver $i_\ell (\ell \in \{1, \cdots, t\})$ extracts her secret decryption key by computing
$$d_{i_\ell} = X_{i_\ell,\ell} h_\ell^{r_{i_\ell,\ell}} \prod_{j=1}^{t,j\neq\ell} X_{i_j,j} h_\ell^{r_{i_j,j}} \prod_{j=t+1}^{n} X_{i_t,j} h_\ell^{r_{i_t,j}}$$
$$= \prod_{j=1}^{t} X_{i_j,j} h_\ell^{r_{i_j,j}} \prod_{j=t+1}^{n} X_{i_t,j} h_\ell^{r_{i_t,j}} = g^x h_\ell^r.$$
Note that $X_{i_\ell,\ell} h_\ell^{r_{i_\ell,\ell}}$ is not published and only the user $i_\ell$ in the receiving list $\mathbb{R}$ can compute it. It is easy to see that $d_{i_\ell}$ satisfies $e(d_{i_\ell}, g) e(h_\ell, R^{-1}) = X$. Hence each user $i_\ell (i_\ell \in \mathbb{R})$ can decrypt the session key $\xi$:
$$e(dk_{i_\ell}, c_1) e(h_\ell, c_2) = e(g^x h_\ell^r, g^\gamma) e(h_\ell, (g^r)^{-\gamma})$$
$$= e(g,g)^{x\gamma} = \xi.$$

As to security, we have the following theorem whose proof is given in the full version of the paper.

THEOREM 2. *Let $\mathcal{A}$ be a semi-static adversary against the above system with advantage $\epsilon$ in time $\tau$. Then, there is an algorithm $\mathcal{B}$ breaking the BDHE assumption with advantage $\epsilon$ in about the same time $\tau$.*

The above construction only achieves semi-static security. However, it can readily be extended to obtain adaptive security by following the conversion in Section 2.2.

### 3.2 Tradeoff between Ciphertexts and Public Keys

The above basic AHBE has constant-size ciphertexts. However, the public key of each user consists of $O(n^2)$ elements and the private key includes $O(n)$ elements. In the following, we illustrate an efficient tradeoff between the public/private keys and ciphertexts.

Let $n = n_1^3$ and we divide the maximal receiver group $\{i_1, \cdots, i_n\}$ into $n_1^2$ subgroups each of which hosts at most $n_1$ receivers. Then we apply our basic AHBE scheme to each subgroup concurrently when a sender wants to broadcast to a set of users $\mathbb{R} \subseteq \{i_1, \cdots, i_n\}$. After employing this approach, the public key of each user consists of $O(n_1^2)$ elements and the secret key contains $O(n_1)$ elements, at a cost that the AHBE ciphertext includes $O(n_1^2)$-size ciphertexts. Hence, the resulting AHBE scheme has sub-linear complexity, i.e., $O(n^{\frac{2}{3}})$ size public keys and ciphertexts, and $O(n^{\frac{1}{3}})$ size private keys. This performance is comparable to the up-to-date conventional broadcast schemes [2] which have sub-linear complexity $O(\sqrt{n})$.

## 4. CONCLUSION

We proposed the notion of AHBE which allows a sender to dynamically broadcast to any *ad hoc* group without the help of a trusted dealer. This primitive provides effective solutions to broadcast applications in emerging ad hoc networks, peer-to-peer networks and other distributed computing environment. We presented the first AHBE schemes which are proven to be adaptively secure in the standard model under the decision BDHE assumption. The resulting scheme enjoys non-interactive decryption and has sub-linear complexity. Our result is comparable to the up-to-date broadcast systems but they require a fully trusted dealer to initialize the system.

## Acknowledgments and Disclaimer

This work is partly supported by the Spanish Government under projects TSI2007-65406-C03-01 "E-AEGIS", TIN2009-11689 "RIPUP", "eVerification" TSI-020100-2009-720, CONSOLIDER INGENIO 2010 CSD2007-00004 "ARES", and by the Government of Catalonia under grant 2009 SGR 1135, and by the NSF of China through projects 60970114, 60970115 and 60970116. The fourth author is partially supported as an ICREA-Acadèmia researcher by the Catalan Government. The authors are with the UNESCO Chair in Data Privacy, but this paper does not necessarily reflect the position of UNESCO nor does it commit that organization.

## 5. REFERENCES

[1] D. Boneh, X. Boyen, E.J. Goh. Hierarchical Identity Based Encryption with Constant Size Ciphertext. In: Cramer, R. (Ed.) *Eurocrypt'05. LNCS*, vol. 3494, pp. 440-456. Springer, Heidelberg, 2005.

[2] C. Gentry, B. Waters. Adaptive Security in Broadcast Encryption Systems (with Short Ciphertexts). In: Joux, A. (ed.) *EUROCRYPT'09. LNCS*, vol. 5479, pp. 171-188. Springer, Heidelberg, 2009.

[3] Q. Wu, Y. Mu, W. Susilo, B. Qin, J. Domingo-Ferrer. Asymmetric Group Key Agreement. In: Joux, A. (ed.) *EUROCRYPT'09, LNCS*, vol. 5479, pp. 153-170. Springer, Heidelberg, 2009.