

Public parameters for
ECDH key exchange

+

ECDH
private key

Alice

=

ECDH
public key

Alice

Public parameters for
ECDH key exchange

+

ECDH
private key

Bob

=

ECDH
public key

Bob

ECDH
public key

Alice

+

ECDH
private key

Bob

=

Secret

Shared

ECDH
public key

Bob

+

ECDH
private key

Alice

=

Secret

Shared

ECDH
public key

Alice

+

ECDH
public key

Bob

=

Garbage

Shared