Diffie-Hellman Key Exchange Implementation

Perry Kundert

2025-01-13:00:00

A critical requirement to support secure decentralized applications, is the ability to compute encryption secrets amongst multiple parties. The Elliptical Curve Diffie-Hellman algorithm supports this, but it must be implemented in Holochain's `lair-keystore`, which stores and manages all cryptographic material for Holochain applications.

For example, to compute some common data between two or more Agents who only know eachother's public keys, the shared data can be derived and used for encryption, but `lair-keystore`'s APIs do not currently allow it to be used to derive shared data for other uses such as independently configuring Holochain DNAs to use a shared DHT, such as required by apps like Volla Messages for two- or multi-party communications. It also prevents the implementation of many types of secure backup schemes involving off-line Ed25519 keypairs held in Crypto hardware wallets or HSMs.

Implements the examples in `https://en.wikipedia.org/wiki/Diffie-Hellman`, and proposes enhancements to `lair-keystore` to support Holochain applications using them.

Contents

1 Two-Party Shared Secrets

A public key is prime modulus of the corresponding private key:

$$A = g^a \bmod p$$
$$B = g^b \bmod p$$

A shared secret calculation has a similar structure:

$$\begin{aligned}
s_{bob} &= A^b \bmod p \\
&= (g^a)^b \\
&= g^{ab} \\
s_{alice} &= B^a \bmod p \\
&= (g^b)^a \\
&= g^{ab}
\end{aligned}$$

1.1 Alice and Bob compute a Shared Secret via Diffie-Hellman

```
def mod_exp(base, exp, modulus):
    """Calculate modular exponentiation efficiently"""
    result = 1
    base = base % modulus
    while exp > 0:
        if exp & 1:
            result = (result * base) % modulus
        base = (base * base) % modulus
        exp >>= 1
    return result

# Public parameters.  Small for demonstration, but cryptographically correct
g = 5   # primitive root
p = 23  # prime modulus

# Private keys
a = 6   # Alice’s private key
b = 15  # Bob’s private key

# Calculate public keys
A = mod_exp(g, a, p)  # Alice’s public key
B = mod_exp(g, b, p)  # Bob’s public key

# Calculate shared secret
s_alice = mod_exp(B, a, p)  # Alice’s calculation
s_bob = mod_exp(A, b, p)    # Bob’s calculation

[
    [ "Party","Private Key","Public Key", "Shared Secret" ],
    None,
    ["Alice", a, A, s_alice],
    ["Bob", b, B, s_bob],
]
```

Party	Private Key	Public Key	Shared Secret
Alice	6	8	2
Bob	15	19	2

1.2 Verify Eve's Known Values

What does Eve the eavesdropper know during this process?

```
[
    [ "Parameter", "Value", "Known to Eve?" ],
    None,
    [ "g", g, "Yes" ],
    [ "p", p, "Yes" ],
    [ "g^a = A", A, "Yes" ],
    [ "g^b = B", B, "Yes" ],
    [ "a", a, "No" ],
    [ "b", b, "No" ],
    [ "g^{ba} = s_{alice}", s_alice, "No"],
    [ "g^{ab} = s_{bob}", s_bob, "No"],
]
```

Parameter	Value	Known to Eve?
g	5	Yes
p	23	Yes
$\mathrm{g}^{\mathrm{a}} = \mathrm{A}$	8	Yes
$\mathrm{g}^{\mathrm{b}} = \mathrm{B}$	19	Yes
a	6	No
b	15	No
$\mathrm{g}^{\mathrm{ba}} = \mathrm{s}_{\mathrm{alice}}$	2	No
$\mathrm{g}^{\mathrm{ab}} = \mathrm{s}_{\mathrm{bob}}$	2	No

2 Three-Party Shared Secret Implementation

For three-party DH, the structure of the intermediate shared secrets is basically the calculation and sharing of values computed by having each party apply their private key exponent the public keys of each of their counterparies, and share this with the one remaining counterparty.

We can assume in many practical scenarios that each party has access to (or is provided with) the public keys of all desired counterparties.

- Public keys are well known, or
- Someone initiates the process by collecting all counterparties' private keys, and sends them to all everyone involved.

However, in this example we'll demonstrate each party creating private keys a, b, c, and transmitting them to all counterparties.

Let's demonstrates that:

- All parties arrive at the same shared secret
- Eve can see all intermediate values but can't compute the final secret
- The implementation follows the two basic principles for extending to larger groups:

1. Starting with g and applying each participant's exponent once (ie. uses their public keys)
2. Each participant applies their private key last to get the final secret

2.1 Computing Intermediate Values and Shared Secret

```
# Private keys
a = 6   # Alice's private key
b = 15  # Bob's private key
c = 13  # Carol's private key

# Calculate public keys (the initial intermediate values)

# Step 1: Alice distributes g^a (her public key, A) to Bob and Carol
A = g_a = mod_exp(g, a, p)
# Bob sends g^b (his public key, B) to Carol and Alice
B = g_b = mod_exp(g, b, p)
# Carol sends g^c to Alice and Bob
C = g_c = mod_exp(g, c, p)

# Step 2: Bob computes (g^a)^b = g^ab and sends to Carol
g_ab = mod_exp(g_a, b, p)
# Carol computes (g^b)^c = g^bc and sends to Alice
g_bc = mod_exp(g_b, c, p)
# Alice computes (g^c)^a = g^ca and sends to Bob
g_ca = mod_exp(g_c, a, p)

# Step 3: Carol computes (g^ab)^c = g^abc = final secret
s_carol = mod_exp(g_ab, c, p)
# Alice computes (g^bc)^a = g^bca = g^abc = final secret
s_alice = mod_exp(g_bc, a, p)
# Bob computes (g^ca)^b = g^cab = g^abc = final secret
s_bob = mod_exp(g_ca, b, p)

[
    ["Party", "Private Key", "Public Key", "Final Secret"],
    None,
    ["Alice", a, A, s_alice],
    ["Bob", b, B, s_bob],
    ["Carol", c, C, s_carol]
]
```

Party	Private Key	Public Key	Final Secret
Alice	6	8	4
Bob	15	19	4
Carol	13	21	4

2.2 What Does Eve Know?

```
[
    ["Intermediate Value", "Expression", "Value", "Known to Eve?"],
    None,
    ["g^a = A", "g^a mod p", g_a, "Yes"],
    ["g^b = B", "g^b mod p", g_b, "Yes"],
    ["g^c = C", "g^c mod p", g_c, "Yes"],
    None,
    ["g^ab = s_{alice/bob}", "g^ab mod p", g_ab, "Yes"],
    ["g^bc = s_{bob/carol}", "g^bc mod p", g_bc, "Yes"],
    ["g^ca = s_{carol/alice}", "g^ca mod p", g_ca, "Yes"],
```

```
    None,
    ["g^abc = s_{alice/bob/carol}", "g^abc mod p", s_carol, "No"]
]
```

Intermediate Value	Expression	Value	Known to Eve?
$\mathrm{g^a = A}$	$\mathrm{g^a}$ mod p	8	Yes
$\mathrm{g^b = B}$	$\mathrm{g^b}$ mod p	19	Yes
$\mathrm{g^c = C}$	$\mathrm{g^c}$ mod p	21	Yes
$\mathrm{g^{ab} = s_{alice/bob}}$	$\mathrm{g^{ab}}$ mod p	2	Yes
$\mathrm{g^{bc} = s_{bob/carol}}$	$\mathrm{g^{bc}}$ mod p	7	Yes
$\mathrm{g^{ca} = s_{carol/alice}}$	$\mathrm{g^{ca}}$ mod p	18	Yes
$\mathrm{g^{abc} = s_{alice/bob/carol}}$	$\mathrm{g^{abc}}$ mod p	4	No

2.3 Verify All Parties Have Same Secret

```
assert s_alice == s_bob == s_carol, "Secrets don't match!"
[
    ["Verification", "Result"],
    None,
    ["All secrets match", "Yes"],
    ["Final shared secret", s_alice]
]
```

Verification	Result
All secrets match	Yes
Final shared secret	4

2.4 Generalizing to N Counterparies

This can extend to as many counterparties as we like. Let's verify this works with 4 parties by adding David (d).

The protocol extends naturally:

- Each party applies their exponent in turn
- The order doesn't matter (verified by calculating two different orders)
- The shared secret remains secure as long as private keys are kept secret

Key mathematical properties:

- The modular exponentiation is associative: $(g^a)^b \bmod p = g^(ab) \bmod p$
  - This allows different computation orders to reach the same final secret
  - The final secret will be $g^{abcd} \bmod p$ regardless of computation order

Security implications:

- Eve would see: $g^a, g^b, g^c, g^d, g^{ab}, g^{bc}, g^{cd}, g^{abc}$
  - But still cannot compute g^{abcd} without knowing at least one private key.

Adding more parties increases the number of visible intermediate values but maintains security *assuming none of the intermediate values are assumed to be secret in any other N-party shared secret computation*!

```
# Parameters
g = 5
p = 23
keys = {
    'a': 6,   # Alice
    'b': 15,  # Bob
    'c': 13,  # Carol
    'd': 17   # David (new)
}

# Calculate 4-party shared secret
# Order: Alice -> Bob -> Carol -> David
g_a = mod_exp(g, keys['a'], p)
g_ab = mod_exp(g_a, keys['b'], p)
g_abc = mod_exp(g_ab, keys['c'], p)
secret1 = mod_exp(g_abc, keys['d'], p)

# Alternative order: David -> Carol -> Bob -> Alice
g_d = mod_exp(g, keys['d'], p)
g_dc = mod_exp(g_d, keys['c'], p)
g_dcb = mod_exp(g_dc, keys['b'], p)
secret2 = mod_exp(g_dcb, keys['a'], p)

[
    ["Shared Secret Verification:"],
    None,
    [ "g^a = A", g_a ],
    [ "g^{ab}", g_ab ],
    [ "g^{abc}", g_abc ],
    [ "Secret via A->B->C->D", secret1],
    None,
    [ "g^d = D", g_d ],
    [ "g^{dc}", g_dc ],
    [ "g^{dcb}", g_dcb ],
    [ "Secret via D->C->B->A", secret2],
    None,
    [ "Secrets match:", secret1 == secret2],
]
```

Shared Secret Verification:	
$g^a = A$	8
g^{ab}	2
g^{abc}	4
Secret via A->B->C->D	2
$g^d = D$	15
g^{dc}	5
g^{dcb}	19
Secret via D->C->B->A	2
Secrets match:	True

Great! But there's an obvious problem... Haven't we seen $g^{ab} = 2$ and $g^{abc} = 4$ somewhere before, as the shared secret between Alice, Bob, and between Alice, Bob and Carol?

3 Shared Secret Exposure Risks

You'll notice that the shared secret $s_{alice/bob} = g^{ab} = 2$ between Alice and Bob using their keypairs $A = g^a$ and $B = g^b$ is **exposed**, if these *same* keypairs are ever used to compute a shared secret between Alice, Bob and anyone else!

So how may we prevent this from ever happening?

3.1 Only Use Long-Term Keys for Two-Party Shared Secrets

The long-term (eg. Agent) keypairs are too useful for encrypting party-to-party communications to avoid using them. This public key is the well-known identity of the agent, and must be reserved for securing communications to and from Agents.

Any implementation must *prevent* the use of long-term keypairs for computing multi-party group secrets.

3.2 Use Single-Purpose Keys for Multi-Party Shared Secrets

When initiating multi-party group shared secret computation, the initiator (say, Alice) must produce a new "group" keypair private key x and public key $g^x = X$ to use as the basis of identifying the group (by the pubic key), and for securely computing the group shared secret.

By Alice sharing this group-specific public key $g^x = X$, *and* by also computing and sharing the first round of intermediate shared values to each counterparty:

$$
\begin{aligned}
g^x &= X \\
g^{ax} &= A^x \\
g^{bx} &= B^x \\
g^{cx} &= C^x
\end{aligned}
$$

everyone can then proceed to compute their first round of intermediate shared secret values, just as for the three-party example. However, since all these intermediate values now depend on a group-unique private exponent x, no information is leaked that can affect any other group shared secret, nor any two-party shared secret.

This example demonstrates how Alice initiates the computation of a group shared secret with Bob and Carol using a group-specific keypair. Here's a breakdown of the process:

```
# Long-term private keys
a = 6  # Alice's private key
b = 15 # Bob's private key
c = 13 # Carol's private key

# Calculate/obtain public keys
A = mod_exp(g, a, p) # Alice's public key
B = mod_exp(g, b, p) # Bob's public key
C = mod_exp(g, c, p) # Carol's public key

# Alice generates a new group-specific private key
x = 19 # Alice's group-specific private key
X = mod_exp(g, x, p) # Alice's group-specific public key

# Alice computes and shares initial intermediate values with everyone for group X
g_ax = mod_exp(A, x, p)
```

```
g_bx = mod_exp(B, x, p)
g_cx = mod_exp(C, x, p)

# Each party computes their first round of intermediate shared secret values, and shares them with
# all other group X counterparties, ignoring any intermediate values containing their own exponent,
# and only sending to counterparties whose exponent is not already included in the value.  Note that
# Alice may receive a redundant copy (g_cxb and g_bxc), so one can be ignored.
g_axb = mod_exp(g_ax, b, p) # Bob's computation, send to Carol
g_cxb = mod_exp(g_cx, b, p) # Bob's computation, send to Alice
g_axc = mod_exp(g_ax, c, p) # Carol's computation, send to Bob
g_bxc = mod_exp(g_bx, c, p) # Carol's computation, send to Alice

# Final shared secret computation
s_alice = mod_exp(g_cxb, a, p)
s_bob = mod_exp(g_axc, b, p)
s_carol = mod_exp(g_axb, c, p)
[
    ["Party", "Public Key", "Intermediate Values", "Final Secret"],
    None,
    ["Group-specific public key (X)", X, "", ""],
    None,
    ["Alice", A, (g_cxb, g_bxc), s_alice],
    ["Bob", B, g_axc, s_bob],
    ["Carol", C, g_axb, s_carol],
    None,
    ["Shared secret match", "", "", s_alice == s_bob == s_carol]
]
```

Party	Public Key	Intermediate Values	Final Secret
Group-specific public key (X)	7		
Alice	8	(11 11)	9
Bob	19	16	9
Carol	21	3	9
Shared secret match			True

4 Implementing in `lair-keystore`

The current implementation of `lair-keystore` is missing a few features required to effectively utilize ECDH (Eliptical Curve Diffie-Hellman) for Two-Party shared secrets, and is support for N-party shared secrets is missing entirely.

These capabilities could be implemented *outside* `lair-keystore` (eg. by using `ed25519-dalek` in the Zome's Rust code), but all keys would need to be generated and managed by the Zome code, losing access to the Agent ID private keys (which are never exposed by `lair-keystore`), and much of the valuable security due to the careful cryptographic secret handling provided by `lair-keystore` – it would be easy to bungle the handling of private keys in Zome code, and expose them unintentionally.

Therefore, I propose the following enhancements to `lair-keystore`:

4.1 Computing Common Shared Data Using a Shared Secret

Many situations involving Agent-to-Agent communications require some shared secret to be computed. This shared secret is computed internally by `lair-keystore` for the local Agents private key and any other Agent's public key.

Presently, arbitrary data can be *encrypted* using `LairApiReqCryptoBoxXSalsaBySignPubKey` etc., by one agent, and can be decrypted by the recipient Agent, which is valuable.

However, there is presently no way for two agents to use this shared secret to compute any other shared data – for example, for two agents to agree on a common Holochain DNA metadata value, so they can independently establish Holochain DNA instances that share the same DHT! Presently, the two Agents must come up with some external mechanism to communicate a common DNA metadata value with each-other, and then establish their DNA instances with the shared DHT.

4.1.1 Enhance `...CryptoBox...` APIs to Allow Optional `nonce`

There are 3 ways that ChaCha20Poly1305 may be safely used by two parties that have arrived at a common shared secret encryption key, with certain constraints:

- Hash some fixed known data with the shared secret, or use it directly as the cipher `key`
- Use 0 or some other shared data (eg. the xor or sort+hash of the two public keys) as `nonce`
- Encrypt known plaintext `data` (eg. zeros) of the desired output length to yield a deterministic shared value between the two Agents

Any of these approaches are valid (do not cryptographically reveal the shared secret) – *if* the `nonce` will never again be used with the same cipher `key` and different plaintext `data`!

It is recommended that some fixed data be hashed with the cipher `key` in this construction, so that if the `nonce` is accidentally reused with the same shared secret cipher `key` and different `data`, it only cryptographically compromises this one application's hashed shared secret – not the valuable single underlying Agent-to-Agent shared secret.

This enhancement is simple, and has limited risk – especially if some additional data is required to hash with the computed Diffie-Hellman shared secret when used as the cipher `key`.

4.2 Revealing Intermediate Values for Multi-Party Shared Secrets

For keypairs stored by `lair-keystore` to be used in computing multi-party shared secrets, at the very least we must implement the ability to provide a value to apply modular exponentiation by a keypair's secret key exponent, and return the result.

This is essentially the procedure for producing a public key from a private key: if the primitive root g is provided, and this function is called for a private key x, the public key X is returned.

If it is called with value of the public key $g^a = A$, using private key x, it would return the shared secret $(g^a)^x = g^{ax}$ derivable by holders of the private keys a and x.

Thus, misuse could easily leak the valuable shared secret used by communications between long-term keypairs of Agents, which `lair-keystore` strives to protect!

Furthermore, the creation of intermediate values during the calculation of shared secrets represent a set of private key exponents (identified by their public keys) in the value. Up until *all* counterparties are represented, multiplying by the private key exponent yields yet another intermediate value to be sent to some counterparty not yet represented in the value. This set of represented keys must be returned along with the intermediate value, and sent along so that the counterparties know the keys included in the value.

However, when all counterparties *are* included in the value, the final modular exponentiation with this Agent's private key exponent yields the **final** shared secret! This secret should be stored by `lair-keystore` encrypted at rest, and *not* returned – it must only be used for subsequent `...CryptoBox...` encryption operations, the same as for two-party shared secrets:

- The encryption of data, with a secure random `nonce`, or
- The production of deterministic shared data, with a user-supplied `nonce` and `data`.

4.2.1 Add `...GroupIntermediate...` APIs To Construct Intermediate Values

Receives a value and a set of Public Keys `represented` and `desired`, and the identity of a locally held private keypair (`ByTag`, `BySignPubKey`, etc.), and:

1. If adding this private key exponent doesn't satisfy all `desired` keys, return the value with the public key added to `represented`.

   The caller then forwards the value and `represented` set along to the appropriate counterparties as an intermediate value.

2. If this is the last key required to fulfill the `desired` keys, then store the shared secret and return a success indicator.

   The caller may then use encryption and decryption operations as for any other computed shared secret, eg. `LairApiReqCryptoBoxXSalsaBySignPubKey`. However, the APIs would have to be enhanced to allow the identification of the shared secret by `desired` group, instead of by `sender_pub_key` and `recipient_pub_key`.

4.3 Implementing in Holochain

Additional APIs must be added to Holochain's `hdk` and `hdi` to allow construction and validation of intermediate values. Once implemented in `lair-keystore`, these should be quite simple.