Noise Explorer: Fully Automated Modeling and Verification for Arbitrary Noise Protocols

Nadim Kobeissi
INRIA Paris
nadim.kobeissi@inria.fr

Karthikeyan Bhargavan
INRIA Paris
karthikeyan.bhargavan@inria.fr

August 23, 2018

Abstract

The Noise Protocol Framework, introduced recently, allows for the design and construction of secure channel protocols by describing them through a simple, restricted language from which complex key derivation and local state transitions are automatically inferred. Noise "Handshake Patterns" can support mutual authentication, forward secrecy, zero round-trip encryption, identity hiding and other advanced features. Since the framework's release, Noise-based protocols have been adopted by WhatsApp, WireGuard and other high-profile applications.

We present Noise Explorer, an online engine for designing, reasoning about and formally verifying arbitrary Noise Handshake Patterns. Based on our formal treatment of the Noise Protocol Framework, Noise Explorer can validate any Noise Handshake Pattern and then translate it into a model ready for automated verification. We use Noise Explorer to analyze 50 Noise Handshake Patterns. We confirm the stated security goals for 12 fundamental patterns and provide precise properties for the rest. We also analyze unsafe Noise patterns and discover potential attacks. All of this work is consolidated into a usable online tool that presents a compendium of results and can parse formal verification results to generate detailed-but-pedagogical reports regarding the exact security guarantees of each message of a Noise Handshake Pattern with respect to each party, under an active attacker and including malicious principals. Noise Explorer evolves alongside the standard Noise Protocol Framework, having already contributed new security goal verification results and stronger definitions for pattern validation and security parameters.

1 Introduction

$$
\begin{array}{l}
IK: \\
\quad \leftarrow s \\
\quad \ldots \\
\quad \rightarrow e, es, s, ss \\
\quad \leftarrow e, ee, se
\end{array}
$$

Figure 1: An example Noise Handshake Pattern, `IK`.

Popular Internet protocols such as SSH and TLS use similar cryptographic primitives: symmetric primitives, public key primitives, one-way hash functions and so forth. Protocol stages are also similarly organized, usually beginning with a authenticated key exchange (AKE) stage followed by a messaging stage. And yet, the design methodology, underlying state machine transitions and key derivation logic tend to be entirely different between protocols with nevertheless similar building blocks. The targeted effective security goals tend to be similar, so why can't the same methodology be followed for everything else?

Standard protocols such as those mentioned above choose a specific set of key exchange protocols to satisfy some stated use-cases while leaving other elements, such as round trips and (notoriously) cipher suites up to the deployer. Specifications use protocol-specific verbose notation to describe the underlying protocol, to the extent that even extracting the core cryptographic protocol becomes hard, let alone analyzing and comparing different modes for security.

Using completely different methodologies to build protocols that nevertheless often share the same primitives and security goals is not only unnecessary, but provably dangerous. The Triple Handshake attack on TLS published in 2014 [1] is based on the same logic that made the attack [2] on the Needham-Schroeder protocol [3] possible almost two decades earlier. The core protocol in TLS 1.2 was also vulnerable to a similar attack, but since the protocol itself is hidden within layers of packet formats and C-like pseudocode, it was difficult for the attack to be detected. However, upon automated symbolic verification [4], the attack quickly appeared not just in TLS, but also in variants of SSH and IPsec. Flaws underlying more recent attacks such as Logjam [5] were known for years before they were observed when the vulnerable protocol was analyzed. Had these protocols differed only in terms of network messages while still using a uniform, formalized logic for internal key derivation and state machine transitioning designed based on the state of the art of protocol analysis, these attacks could have been avoided.

1.1 The Noise Protocol Framework

The Noise Protocol Framework [6], recently introduced by Trevor Perrin, aims to avert this problem by presenting a simple language for describing cryptographic network protocols. In turn, a large number of semantic rules extend this simple protocol description to provide state machine transitions, key derivation logic and so on. The goal is to obtain the strongest possible effective security guarantees for a given protocol based on its description as a series of network messages by deriving its other elements from a uniform, formally specified logic followed by all protocol designs.

In designing a new secure channel protocol using the Noise Protocol Framework, one only provides an input using the simple language shown in Fig. 1. As such, from the viewpoint of the protocol designer, Noise protocols can only differ in the number of messages, the types of keys exchanged and the sequence or occurrence of public key transmissions and Diffie-Hellman operations. Despite the markedly non-expressive syntax, however, the occurence and position of the “tokens” in each message pattern can trigger complex state machine evolutions for both parties, which include operations such as key derivation and transcript hash mixing.

Let’s examine Fig. 1. Before the AKE begins, the responder shares his static public key. Then in the first protocol message, the initiator sends a fresh ephemeral key, calculates a Diffie-Hellman shared secret between her ephemeral key and the recipient’s public static key, sends her public static key and finally calculates a Diffie-Hellman shared secret between her static key and the responder’s public static key. The responder then answers by generating an ephemeral key pair and sending his ephemeral public key, deriving a Diffie-Hellman shared secret between his ephemeral key and the ephemeral key of the initiator and another Diffie-Hellman shared secret between his static key and the ephemeral key of the initiator. Both of these AKE messages can also contain message payloads, which, depending on the availability of sufficient key material, could be AEAD-encrypted (in this particular Noise Handshake Pattern, this is indeed the case.)

As we can see, quite a few operations have occured in what would at first glance appear to be simple syntax for a simple protocol. Indeed, underlying these operations is a sophisticated state machine logic tasked with mixing all of the derived keys together, determining when it is safe (or possible) to send encrypted payloads and ensuring transcript consistency, among other things. This is the value of the Noise Protocol Framework: allowing the protocol designer to describe what they need their protocol to do fairly effectively using this simple syntax, and leaving the rest to a sturdy set of underlying rules.

1.2 Noise Explorer: Formal Verification for any Noise Handshake Pattern

Noise Explorer, the central contribution of this work, capitalizes on the strengths of the Noise Protocol Framework in order to allow for automated protocol verification to no longer be limited only to monolithic, pre-defined protocols with their own notation. In this work, we formalize Noise’s syntax, semantics, state transitions and Noise Handshake Pattern validity rules. We then present translation logic to go from Noise Handshake Patterns directly into full symbolic models ready for automated verification using ProVerif [7, 8].

This allows us to then construct Noise Explorer, an online engine that allows for designing, validating and subsequently generating cryptographic models for the automated formal verification of any arbitrary

Noise Handshake Pattern. Models generated using Noise Explorer allow for the verification of Noise-based secure channel protocols against a battery of comprehensive and sophisticated security queries. Noise Explorer also comes with the first compendium of formal verification results for Noise Handshake Patterns, browsable online using an interactive web application that presents dynamically generated diagrams indicating with strong precision every cryptographic operation and security guarantee relevant to every message within the Noise Handshake Pattern.

1.3 Contributions

Formal semantics and validity rules for Noise Handshake Patterns. §2 introduces the Noise Protocol Framework in detail, presenting the first formal semantics and validity rules (illustrated as typing inference rules) for Noise Handshake Patterns. This allows Noise Explorer to validate and separate sane Noise Handshake Patterns from invalid ones based on arbitrary input, and is the foundation of further contributions described below.

Translations from Noise Patterns to processes in the applied-pi calculus. §3 discusses automated translations from valid Noise Handshake Patterns into a representation in the applied-pi calculus [9] which includes cryptographic primitives, state machine transitions, message passing and a top-level process illustrating live protocol execution.

Noise security querized formalized as security goals. In §4, we model all five "confidentiality" security goals from the Noise Protocol Framework specification in the applied-pi calculus and extend the two "authentication" goals to four.

Formal verification results for 50 Noise Handshake Patterns in the Noise Protocol Framework specification. §5 sees all of the previous contributions come together to provide formal verification results for 50 Noise Handshake Patterns.[1] We find that while most of the results match those predicted by the specification authors, our extended model for "authentication" queries allows for more nuanced results. Furthermore, we analyze unsafe Noise Handshake Patterns and discover a potential for forgery attacks.

1.4 Related Work

This work represents the first comprehensive formal analysis of the Noise Protocol Framework. However, substantial tangential work has occured centering on the WireGuard [10] VPN protocol, which employs the `IKpsk2` Noise Handshake Pattern: Lipp [11] presented an automated computational proof of WireGuard, Donenfeld et al [12] presented an automated symbolic verification of WireGuard and Dowling et al [13] presented a hand proof of WireGuard. These analyses' results on the `IKpsk2` handshake pattern were in line with those we found in our own symbolic analysis. Other work exists centering on the automated verification of modern protocols [14, 15].

2 The Noise Protocol Framework

Noise's protocol description language is restricted only to describing messages between two parties (initiator and responder), the public keys communicated and any Diffie-Hellman operations conducted. Messages are called Noise "Message Patterns". They make up authenticated key exchanges, which are called Noise "Handshake Patterns". Noise supports authenticated encryption with added data (AEAD) and Diffie-Hellman key agreement. Noise does not support any signing operations.

The full description of a Noise protocol is contained within its description of a Noise Handshake Pattern, such as the one seen in Fig. 1. The initial messages within a Noise Handshake Pattern, which contain *tokens* representing public keys or Diffie-Hellman operations is called a *handshake message*. After handshake messages, *transport messages* may occur carrying encrypted payloads. Here is an overview of the tokens that may appear in a handshake message:

[1] Anyone can use Noise Explorer to increase this number by designing, validating then automatically verifying their own Noise Handshake Pattern.

- `e, s` The sender is communicating their ephemeral or static public key, respectively.
- `ee, es, se, ss` The sender has locally calculated a new shared secret. The first letter of the token indicates the initiator's key share while the second indicates the responder's key share. As such, this token remains the same irrespective of who is sending the particular handshake message in which it occurs.
- `psk` The sender is mixing a pre-shared key into their local state and the recipient is assumed to do the same.

Optionally, certain key materials can be communicated before a protocol session is initiated. A practical example of how this is useful could be secure messaging protocols, where prior knowledge of an ephemeral key pair could help a party initiate a session using a zero-round-trip protocol, which allows them to send an encrypted payload without the responder needing to be online.

These *pre-message patterns* are represented by a series of messages occuring before handshake messages. The end of the pre-message stage is indicated by a "..." sign. For example, in Fig. 1, we see a pre-message pattern indicating that the initiator has prior knowledge of the responder's public static key before initiating a protocol session.

We consider the following validity rules on Noise Handshake Patterns:

- **Alternating message directions.** Message direction within a Noise Handshake Pattern must alternate (initiator $\rightarrow$ responder, initiator $\leftarrow$ responder), with the first message being sent by the initiator.
- **Performing Diffie-Hellman key agreement more than once.** Principals must not perform the same Diffie-Hellman key agreement more than once per handshake.[2]
- **Sending keys more than once.** Principals must not send their static public key or ephemeral public key more than once per handshake.
- **Transport messages after handshake messages.** Noise Handshake Patterns can only contain transport handshake messages at the very bottom of the pattern.
- **Appropriate key share communication.** Principals cannot perform a Diffie-Hellman operation with a key share that was not communicated to them prior.
- **Unused key shares.** Noise Handshake Patterns should not contain key shares that are not subsequently used in any Diffie-Hellman operation.
- **Transport messages.** Noise Handshake Patterns cannot consist purely of transport messages.

2.1 Cryptographic Primitives

Noise Handshake Patterns make use of cryptographic primitives which in this work we will treat as constructions in the symbolic model. As such, only their effective security guarantees are relevant; computational details such as bit length are not carried over from the Noise Protocol Framework specification. This is further explained in §4.

We consider the following cryptographic primitives:

- $KP()$**:** Generates a new Diffie-Hellman key pair consisting of a private key x and a public key g^x.
- $DH(x \leftarrow KP(), y)$**:** Derives a Diffie-Hellman shared secret between the private key within the key pair x and the public key y.

[2]This rule is not currently specified concretely although it is strongly implied in the specification. We assume it for completeness.

Validity Rules

$d ::= \leftarrow \mid \rightarrow$	*direction*: left or right
$\bar{t} ::= k^d \mid k_1k_2 \mid psk$	tokens with directed DH keys
$\Gamma ::= \{\bar{t}_0, \ldots, \bar{t}_n\}$	*context*: set of prior tokens

$$tokens^d(m) \triangleq \{k^d \mid k \in m \cap \{e,s\}\} \cup (m \setminus \{e,s\})$$

$$\boxed{\text{Pre-Message Validity: } \Gamma \vdash^d p}$$

$$\text{PreEmpty}\ \frac{}{\Gamma \vdash^d \epsilon}$$

$$\text{PreKey}\ \frac{k^d \notin \Gamma \quad \Gamma \cup \{k^d\} \vdash^d p}{\Gamma \vdash^d k, p}$$

$$\boxed{\text{Message Validity: } \Gamma \vdash^d m}$$

$$\text{MsgEmpty}^{\rightarrow}\ \frac{\begin{array}{c} ss \in \Gamma \Rightarrow se \in \Gamma \quad se \in \Gamma \Rightarrow ee \in \Gamma \\ psk \in \Gamma \Rightarrow e^{\rightarrow} \in \Gamma \end{array}}{\Gamma \vdash^{\rightarrow} \epsilon}$$

$$\text{MsgEmpty}^{\leftarrow}\ \frac{\begin{array}{c} ss \in \Gamma \Rightarrow es \in \Gamma \quad es \in \Gamma \Rightarrow ee \in \Gamma \\ psk \in \Gamma \Rightarrow e^{\leftarrow} \in \Gamma \end{array}}{\Gamma \vdash^{\leftarrow} \epsilon}$$

$$\text{MsgKey}\ \frac{k^d \notin \Gamma \quad \Gamma \cup \{k^d\} \vdash^d m}{\Gamma \vdash^d k, m}$$

$$\text{MsgDH}\ \frac{\begin{array}{c} k_1^{\rightarrow} \in \Gamma \quad k_2^{\leftarrow} \in \Gamma \quad k_1k_2 \notin \Gamma \\ \Gamma \cup \{k_1k_2\} \vdash^d m \end{array}}{\Gamma \vdash^d k_1k_2, m}$$

$$\text{MsgPSK}\ \frac{psk \notin \Gamma \quad \Gamma \cup \{psk\} \vdash^d m}{\Gamma \vdash^d psk, m}$$

$$\boxed{\text{Handshake Validity: } \Gamma \vdash h_i}$$

$$\text{HSEmpty}\ \frac{}{\Gamma \vdash \epsilon}$$

$$\text{HSMessageI}\ \frac{\Gamma \vdash^{\rightarrow} m \quad \Gamma \cup tokens^{\rightarrow}(m) \vdash h_r}{\Gamma \vdash \xrightarrow{m} h_r}$$

$$\text{HSMessageR}\ \frac{\Gamma \vdash^{\leftarrow} m \quad \Gamma \cup tokens^{\leftarrow}(m) \vdash h_i}{\Gamma \vdash \xleftarrow{m} h_i}$$

$$\boxed{\text{Noise Pattern Validity: } \vdash n}$$

$$\text{NoiseValid}\ \frac{\begin{array}{c} \{\} \vdash^{\rightarrow} p_1 \quad \{\} \vdash^{\leftarrow} p_2 \\ tokens^{\rightarrow}(p_1) \cup tokens^{\leftarrow}(p_2) \vdash h_i \end{array}}{\vdash \xrightarrow{p_1} \xleftarrow{p_2} h_i}$$

Figure 2: Noise Pattern Validity Rules

- $E(k, n, ad, p)$**:** Encrypts and generates an authentication tag for plaintext p using key k and nonce n, optionally extending the authentication tag to cover added data ad. The output is considered to be Authenticated Encryption with Added Data (AEAD) [16].
- $D(k, n, ad, c)$**:** Decrypts and authenticates ciphertext c using key k and nonce n. Added data ad must also be included if it was defined during the encryption step for authentication to pass on both c and ad.
- $R(k)$**:** Returns a new key by applying a pseudorandom function on k.
- $H(d)$**:** A one-way hash function on data d.
- $HKDF(ck, ik)$**:** A Hash-Based Key Derivation function [17] that takes keys (ck, ik) and outputs a triple of keys. In some instances, the third key output is discarded and not used. The function is similar to the original HKDF definition but with ck acting as the salt and with a zero-length *"info"* variable.

In the ProVerif automated protocol verification framework, Diffie-Hellman is implemented as a `letfun` that takes two `key`-type values (representing points on X25519 [18] elliptic curve) along with an `equation` that essentially illustrates the Diffie-Hellman relationship $g^{ab} = g^{ba}$ in the symbolic model.[3] DH and KP (implemented as `generate_keypair`) are then implemented as `letfuns` on top of that construction:[4]

[3]Recall that, in the symbolic model, any arithemtic property such as additivity is not a given and must be modeled specifically.

[4]`keypairpack` and `keypairunpack` are a `fun` and `reduc` pair that allow compressing and decompressing a tuple of `key` values into a `keypair`-type value for easy handling throughout the model. Whenever the suffixes `pack` and `unpack` appear from now on, it is safe to assume that they function in a similar pattern.

```
fun dhexp(key, key):key.
equation forall a:key, b:key;
      dhexp(b, dhexp(a, g)) = dhexp(a, dhexp(b, g)).
```

Encryption is implemented as a function that produces a bitstring (representing the ciphertext) parametrized by a key, nonce, added data and plaintext. Decryption is a reduction function that produces the correct plaintext only when the appropriate parameters are given, otherwise the process ends:

```
fun encrypt(key, nonce, bitstring, bitstring):bitstring.

fun decrypt(key, nonce, bitstring, bitstring):aead reduc
      forall k:key, n:nonce, ad:bitstring, plaintext:bitstring;
            decrypt(k, n, ad, encrypt(k, n, ad, plaintext)) = aeadpack(true, ad, plaintext).
```

Finally, H and $HMAC$ are implemented as one-way functions parametrized by two bitstrings (for ease of use in modeling in the case of H, and for a keyed hash representation in the case of $HMAC$) while $HKDF$ is constructed on top of them.

2.2 Local State

Each principal in a Noise protocol handshake keeps three local state elements: `CipherState`, `SymmetricState` and `HandshakeState`. These states contain each other in a fashion similar to a Russian Matryoshka doll, with `HandshakeState` being the largest element, containing `SymmetricState` which in turn contains `CipherState`.

- **`CipherState`** contains k and n, symmetric keys used to encrypt and decrypt ciphertexts.
- **`SymmetricState`** contains a `CipherState` tuple (k, n), an additional key ck and a hash function output h.
- **`HandshakeState`** contains a `SymmetricState` along with additional local public keys (s, e) and remote public keys (rs, re).

Each state element comes with its own set of state transformation functions. These functions are triggered by the occurence and position of tokens within a Noise Handshake Pattern. We present a description of the state transition functions as seen in the Noise Protocol Framework specification, but restricted to a representation that follows implementing Noise Handshake Patterns in the symbolic model.

2.2.1 CipherState

A `CipherState` comes with the following state transition functions:

- **`InitializeKey(key):`** Sets $k =$ `key`. Sets $n = 0$.
- **`HasKey():`** Returns true if k is non-empty, false otherwise.
- **`SetNonce(nonce):`** Sets $n =$ `nonce`.
- **`EncryptWithAd(ad, p):`** If k is non-empty returns $E(k, n, ad, p)$ then increments n. Otherwise returns p.
- **`DecryptWithAd(ad, c):`** If k is non-empty returns $D(k, n, ad, c)$ then increments n. Otherwise returns c. n is not incremented if authenticated decryption fails.
- **`Rekey():`** Sets $k = R(k)$.

In ProVerif, `InitializeKey` simply returns a `cipherstate`-type value packed with the input key and a starting nonce. `hasKey` unpacks an input `cipherstate` and checks whether the key is defined. The rest of the functions are based on similarly evident constructions:

```
letfun encryptWithAd(cs:cipherstate, ad:bitstring, plaintext:bitstring) =
      let (k:key, n:nonce) = cipherstateunpack(cs) in
      let e = encrypt(k, n, ad, plaintext) in
      let csi = setNonce(cs, increment_nonce(n)) in
      (csi, e).

letfun decryptWithAd(cs:cipherstate, ad:bitstring, ciphertext:bitstring) =
      let (k:key, n:nonce) = cipherstateunpack(cs) in
      let d = decrypt(k, n, ad, ciphertext) in
      let (valid:bool, adi:bitstring, plaintext:bitstring) = aeadunpack(d) in
      let csi = setNonce(cs, increment_nonce(n)) in
      (csi, plaintext, valid).

letfun reKey(cs:cipherstate) =
      let (k:key, n:nonce) = cipherstateunpack(cs) in
      let ki = encrypt(k, maxnonce, empty, zero) in
      cipherstatepack(bit2key(ki), n).
```

2.2.2 SymmetricState

A `SymmetricState` comes with the following state transition functions:

- **`InitializeSymmetric(name)`:** Sets $ck = h = H(\texttt{name})$.
- **`MixKey(ik)`:** Sets $(ck, tk) = HKDF(ck, \texttt{ik})$ and calls $InitializeKey(tk)$.
- **`MixHash(data)`:** Sets $h = H(h \parallel \texttt{data})$.[5]
- **`MixKeyAndHash(ik)`:** Sets $(ck, th, tk) = HKDF(ck, \texttt{ik})$, then calls `MixHash`$(th)$ and `InitializeKey`(tk).
- **`GetHandshakeHash()`:** Returns h.
- **`EncryptAndHash(p)`:** Sets $c =$ `EncryptWithAd`$(h, \texttt{p})$. Calls $MixHash(c)$ and returns c.
- **`DecryptAndHash(c)`:** Sets $p =$ `DecryptWithAd`$(h, \texttt{c})$ and returns p.
- **`Split()`:** Sets $(tk_1, tk_2) = HKDF(ck, \texttt{zero})$. Creates two `CipherStates` (c_1, c_2). Calls c_1`.InitializeKey`(tk_1) and c_2`.InitializeKey`(tk_2). Returns (c_1, c_2), a pair of `CipherStates` for encrypting transport messages.[6]

In ProVerif, these functions are implemented based on `letfun` declarations that combine previously declared `funs` and `letfuns`:

```
      letfun initializeSymmetric(protocol_name:bitstring) =
      let h = hash(protocol_name, empty) in
      let ck = bit2key(h) in
      let cs = initializeKey(bit2key(empty)) in
      symmetricstatepack(cs, ck, h).

letfun mixKey(ss:symmetricstate, input_key_material:key) =
      let (cs:cipherstate, ck:key, h:bitstring) = symmetricstateunpack(ss) in
      let (ck:key, temp_k:key, output_3:key) = hkdf(ck, input_key_material) in
      symmetricstatepack(initializeKey(temp_k), ck, h).

letfun mixHash(ss:symmetricstate, data:bitstring) =
      let (cs:cipherstate, ck:key, h:bitstring) = symmetricstateunpack(ss) in
      symmetricstatepack(cs, ck, hash(h, data)).

letfun mixKeyAndHash(ss:symmetricstate, input_key_material:key) =
      let (cs:cipherstate, ck:key, h:bitstring) = symmetricstateunpack(ss) in
      let (ck:key, temp_h:key, temp_k:key) = hkdf(ck, input_key_material) in
```

[5] $\parallel$ denotes bitstring concatenation.
[6] `zero` is meant to denote a null bitstring.

```
        let (cs:cipherstate, temp_ck:key, h:bitstring) = symmetricstateunpack(mixHash(
            symmetricstatepack(cs, ck, h), key2bit(temp_h))) in
        symmetricstatepack(initializeKey(temp_k), ck, h).

letfun getHandshakeHash(ss:symmetricstate) =
        let (cs:cipherstate, ck:key, h:bitstring) = symmetricstateunpack(ss) in
        (ss, h).

letfun encryptAndHash(ss:symmetricstate, plaintext:bitstring) =
        let (cs:cipherstate, ck:key, h:bitstring) = symmetricstateunpack(ss) in
        let (cs:cipherstate, ciphertext:bitstring) = encryptWithAd(cs, h, plaintext) in
        let ss = mixHash(symmetricstatepack(cs, ck, h), ciphertext) in
        (ss, ciphertext).

letfun decryptAndHash(ss:symmetricstate, ciphertext:bitstring) =
        let (cs:cipherstate, ck:key, h:bitstring) = symmetricstateunpack(ss) in
        let (cs:cipherstate, plaintext:bitstring, valid:bool) = decryptWithAd(cs, h, ciphertext
            ) in
        let ss = mixHash(symmetricstatepack(cs, ck, h), ciphertext) in
        (ss, plaintext, valid).

letfun split(ss:symmetricstate) =
        let (cs:cipherstate, ck:key, h:bitstring) = symmetricstateunpack(ss) in
        let (temp_k1:key, temp_k2:key, temp_k3:key) = hkdf(ck, bit2key(zero)) in
        let cs1 = initializeKey(temp_k1) in
        let cs2 = initializeKey(temp_k2) in
        (ss, cs1, cs2).
```

2.2.3 HandshakeState

A `HandshakeState` comes with the following state transition functions:

- **`Initialize(hp, i, s, e, rs, re)`:** hp denotes a valid Noise Handshake Pattern. i is a boolean which denotes whether the local state belongs to the initiator. Public keys (s, e, rs, re) may be left empty or may be pre-initialized in the event that any of them appeared in a pre-message. Calls `InitializeSymmetric(hp.name)`. Calls `MixHash()` once for each public key listed in the pre-messages within `hp`.

- **`WriteMessage(p)`:** Depending on the tokens present in the current handshake message, different operations occur:

  - e: Sets $e \leftarrow KP()$. Appends g^e to the return buffer. Calls `MixHash`(g^e).
  - s: Appends `EncryptAndHash`(g^s) to the buffer.
  - ee: Calls `MixKey`$(DH(e, re))$.
  - es: Calls `MixKey`$(DH(e, rs))$ if initiator, `MixKey`$(DH(s, re))$ if responder.
  - se: Calls `MixKey`$(DH(s, re))$ if initiator, `MixKey`$(DH(e, rs))$ if responder.
  - ss: Calls `MixKey`$(DH(s, rs))$.

  Then, `EncryptAndHash(p)` is appended to the return buffer. If there are no more handshake messages, two new `CipherStates` are returned by calling `Split()`.

- **`ReadMessage(m)`:** Depending on the tokens present in the current handshake message, different operations occur:

  - e: Sets `re` to the public ephemeral key retrieved from `m`.
  - s: Sets `temp` to the encrypted public static key retrieved from `m`. Sets `rs` to the result of `DecryptAndHash(temp)`, failing on authenticated decryption error.
  - ee: Calls `MixKey`$(DH(e, re))$.
  - es: Calls `MixKey`$(DH(e, rs))$ if initiator, `MixKey`$(DH(s, re))$ if responder.

  - *se*: Calls `MixKey`$(DH(s, re))$ if initiator, `MixKey`$(DH(e, rs))$ if responder.
  - *ss*: Calls `MixKey`$(DH(s, rs))$.

  Then, `DecryptAndHash` is called on the message payload extracted from m. If there are no more handshake messages, two new `CipherStates` are returned by calling `Split()`.

The translation of `HandshakeState` functions in ProVerif is generated dynamically and differs by model. Hence, we discuss them in more detail in §3.

2.3 Security Grades

The Noise Protocol Framework specification defines different Noise Handshake Patterns to suit different scenarios. These patterns come with different security properties depending on which keys and shared secrets are employed and when. Two types of security grades are defined: *"authentication"* grades dealing with the authentication of a message to a particular sender (and optionally, receiver) and *"confidentiality"* grades dealing with a message's ability to resist the obtention of plaintext by an unauthorized party.

Authentication grades are defined in the original specification as follows:

- **Grade 0: No authentication.** This payload may have been sent by any party, including an active attacker.
- **Grade 1: Sender authentication vulnerable to key-compromise impersonation (KCI).** The sender authentication is based on a static-static Diffie-Hellman key share (*ss*) involving both parties' static key pairs. If the recipient's long-term private key has been compromised, this authentication can be forged.
- **Grade 2: Sender authentication resistant to key-compromise impersonation (KCI).** The sender authentication is based on an ephemeral-static Diffie-Hellman key share (*es* or *se*) between the sender's static key pair and the recipient's ephemeral key pair. Assuming the corresponding private keys are secure, this authentication cannot be forged.

Confidentiality grades are defined in the original specification as follows:

- **Grade 0: No confidentiality.** This payload is sent in cleartext.
- **Grade 1: Encryption to an ephemeral recipient.** This payload has forward secrecy, since encryption involves an ephemeral-ephemeral Diffie-Hellman key share (*ee*). However, the sender has not authenticated the recipient, so this payload might be sent to any party, including an active attacker.
- **Grade 2: Encryption to a known recipient, forward secrecy for sender compromise only, vulnerable to replay.** This payload is encrypted based only on DHs involving the recipient's static key pair. If the recipient's static private key is compromised, even at a later date, this payload can be decrypted. This message can also be replayed, since there's no ephemeral contribution from the recipient.
- **Grade 3: Encryption to a known recipient, weak forward secrecy.** This payload is encrypted based on an ephemeral-ephemeral Diffie-Hellman key share and also an ephemeral-static Diffie-Hellman key share involving the recipient's static key pair. However, the binding between the recipient's alleged ephemeral public key and the recipient's static public key hasn't been verified by the sender, so the recipient's alleged ephemeral public key may have been forged by an active attacker. In this case, the attacker could later compromise the recipient's static private key to decrypt the payload.
- **Grade 4: Encryption to a known recipient, weak forward secrecy if the sender's private key has been compromised.** This payload is encrypted based on an ephemeral-ephemeral Diffe-Helllman key share and also based on an ephemeral-static Diffie-Hellman key share involving the

recipient's static key pair. However, the binding between the recipient's alleged ephemeral public and the recipient's static public key has only been verified based on DHs involving both those public keys and the sender's static private key. Thus, if the sender's static private key was previously compromised, the recipient's alleged ephemeral public key may have been forged by an active attacker. In this case, the attacker could later compromise the intended recipient's static private key to decrypt the payload.

- **Grade 5: Encryption to a known recipient, strong forward secrecy.** This payload is encrypted based on an ephemeral-ephemeral Diffie-Hellman key share as well as an ephemeral-static Diffie-Hellman key share with the recipient's static key pair. Assuming the ephemeral private keys are secure, and the recipient is not being actively impersonated by an attacker that has stolen its static private key, this payload cannot be decrypted.

$$\begin{aligned} &IN: \\ &\qquad \rightarrow e, s \\ &\qquad \leftarrow e, ee, se \end{aligned}$$

Figure 3: An example Noise Handshake Pattern, `IN`.

The Noise Handshake Pattern illustrated in Fig. 1 is described in the original specification as claiming strong security guarantees: Handshake and transport message are attributed authentication grades of 1, 2, 2 and 2 respectively, and confidentiality grades of 2, 4, 5 and 5. Other Noise Handshake Patterns, such as the one described in Fig. 3, sacrifice security properties to deal away with the need to share public keys beforehand or to conduct additional key derivation steps (authentication: 0, 0, 2, 0 and confidentiality: 0, 3, 1 5.)

In our analysis, we leave the confidentiality grades intact. However, we introduce two new additional security grades, 3 and 4, which provide more nuance for the existing authentication grades 1 and 2. In our analysis, authentication grades 1 and 2 hold even if the authentication of the message can be forged towards the recipient if the sender carries out a separate session with a separate, compromised recipient. authentication grades 3 and 4 do not hold in this case. This nuance does not exist in the authentication grades defined in the latest Noise Protocol Framework specification. Security grades are formalized and explored in more detail in §4.

2.4 Other Specification Features

The Noise Protocol Framework specification defines 15 "fundamental patterns", 23 "deferred patterns" and 21 "PSK patterns". `IK` (Fig. 1) and `IN` (Fig. 3) are two fundamental patterns. Deferred patterns are essentially modified fundamental patterns where the communication of public keys or the occurence of Diffie-Hellman operations is intentionally delayed. PSK pattterns are patterns in which a pre-shared key token appears. Fig. 4 illustrates a deferred pattern based on the fundamental pattern shown in Fig. 1.

The full Noise Protocol Framework specification extends somewhat beyond the description given as part of this work, including features such as "identity hiding" and "dummy keys." Some of these features were not considered due to them not being relevant to a formal symbolic analysis, while others, such as identity hiding, which tests for whether a Noise Handshake Pattern leaks the long-term identity of principals to different types of attackers, are potentially valuable and slated as future work.

$$\begin{aligned} &I1K: \\ &\qquad \leftarrow s \\ &\qquad \ldots \\ &\qquad \rightarrow e, es, s \\ &\qquad \leftarrow e, ee \\ &\qquad \rightarrow se \end{aligned}$$

Figure 4: An example Noise Handshake Pattern, `I1K`. This is a deferred pattern based on `IK`, shown in Fig. 1.

3 Translating Noise Protocols to the Applied-Pi Calculus

Based on our description of the Noise Protocol Framework in §2, we develop a set of rules and constructions to automatically translate Noise Handshake Patterns into formal models. As mentioned in §1, we

```
letfun writeMessage_a(me:principal, them:principal, hs:handshakestate, payload:bitstring, sid:sessionid) =
let (ss:symmetricstate, s:keypair, e:keypair, rs:key, re:key, psk:key, initiator:bool) = handshakestateunpack(hs) in
let (ne:bitstring, ciphertext1:bitstring, ciphertext2:bitstring) = (empty, empty, empty) in
let e = generate_keypair(key_e(me, them, sid)) in
let ne = key2bit(getpublickey(e)) in
let ss = mixHash(ss, ne) in
(* No PSK, so skipping mixKey *)
let ss = mixKey(ss, dh(e, rs)) in
let s = generate_keypair(key_s(me)) in
let (ss:symmetricstate, ciphertext1:bitstring) = encryptAndHash(ss, key2bit(getpublickey(s))) in
let ss = mixKey(ss, dh(s, rs)) in
let (ss:symmetricstate, ciphertext2:bitstring) = encryptAndHash(ss, payload) in
let hs = handshakestatepack(ss, s, e, rs, re, psk, initiator) in
let message_buffer = concat3(ne, ciphertext1, ciphertext2) in
(hs, message_buffer).
```

```
letfun readMessage_a(me:principal, them:principal, hs:handshakestate, message:bitstring, sid:sessionid) =
let (ss:symmetricstate, s:keypair, e:keypair, rs:key, re:key, psk:key, initiator:bool) = handshakestateunpack(hs) in
let (ne:bitstring, ciphertext1:bitstring, ciphertext2:bitstring) = deconcat3(message) in
let valid1 = true in
let re = bit2key(ne) in
let ss = mixHash(ss, key2bit(re)) in
(* No PSK, so skipping mixKey *)
let ss = mixKey(ss, dh(s, re)) in
let (ss:symmetricstate, plaintext1:bitstring, valid1:bool) = decryptAndHash(ss, ciphertext1) in
let rs = bit2key(plaintext1) in
let ss = mixKey(ss, dh(s, rs)) in
let (ss:symmetricstate, plaintext2:bitstring, valid2:bool) = decryptAndHash(ss, ciphertext2) in
if ((valid1 && valid2) && (rs = getpublickey(generate_keypair(key_s(them))))) then (
      let hs = handshakestatepack(ss, s, e, rs, re, psk, initiator) in
      (hs, plaintext2, true)).
```

Figure 5: The `WriteMessage` and `ReadMessage` `letfun` constructions for the first message in `IK` (Fig. 1), generated according to translation rules from Noise Handshake Pattern to ProVerif. The appropriate state transition functions are invoked in accordance with the occurence and ordering of tokens in the message pattern.

use the ProVerif automated protocol verifier to obtain answers to our security queries. ProVerif uses the applied-pi calculus, an ML-like language geared towards the description of network protocols, as its input language. It analyzes described protocols under a Dolev-Yao model, which effectively mimicks an active network attacker. ProVerif models are comprised of a section in which cryptographic protocol primitives and operations are described as `funs` or `letfuns` and a "top-level process" section in which the execution of the protocol on the network is outlined. Parallel and unbounded numbers of executions of different parts of the protocol are supported.

In the symbolic model, cryptographic primitives are "black boxes": encryption functions are pseudorandom permutations, hash functions are perfect one-way functions and so on. *Computational* details such as a hash function's vulnerability to length extension attacks are not considered.

3.1 ProVerif Model Components

In the ProVerif model of a Noise Handshake Pattern, there are nine components:

1. **ProVerif parameters.** This includes whether to reconstruct a trace and whether the attacker is active or passive.

2. **Types.** Cryptographic elements, such as keys are nonces, are given types. `CipherStates`, `SymmetricStates` and `HandshakeStates` are given types as well as constructors and reductors.

3. **Constants.** The generator of the g Diffie-Hellman group, HKDF constants such as `zero` and the names of principals (Alice, indicating the initiator, Bob, indicating the recipient, and Charlie, indicating a compromised principal controlled by the attacker) are all declared as constants.

4. **Bitstring concatenation.** Functions are declared for bitstring concatenation, useful for constructing and destructing the message buffers involved in `WriteMessage` and `ReadMessage`.
5. **Cryptographic primitives.** DH, KP, E, D, H and $HKDF$ (all described in §2) are modeled as cryptographic primitives in the symbolic model.
6. **State transition functions.** All functions defined for `CipherState`, `SymmetricState` and `HandshakeState` are implemented in the applied-pi calculus.
7. **Channels.** Only a single channel is declared, `pub`, representing the public Internet.
8. **Events and queries.** Here, the protocol events and security queries relevant to a particular Noise Handshake Pattern are defined. This includes the four authentication queries and five confidentiality queries introduced in §2.
9. **Protocol processes and top-level process.** This includes the `WriteMessage` and `ReadMessage` function for each handshake and transport message, followed by the top-level process illustrating the live execution of the protocol on the network.

3.2 Verification Context

All generated models execute the protocol in a highly comprehensive context for verification: Alice initiates a session with Bob, a process in which Alice initiates a session with Charlie, a process in which Bob acts a responder to Alice and a process in which Bob acts as a responder to Charlie. Charlie is a compromised participant whose entire state is controlled by the attacker. Each process in the top-level process are executed in parallel. The top-level process is executed in an unbounded number of sessions. Within the processes, transport messages are again executed in an unbounded number of sessions in both directions. Fresh key material is provided for each ephemeral generated in each session within the unbounded number of sessions: no ephemeral key reuse occurs between the sessions modeled.

3.3 Translation

Most of the cryptographic primitives and state transition functions, are included from a pre-existing set of Noise Protocol Framework ProVerif headers written as a part of this work and are not automatically generated according to a set of rules. Events, queries, protocol processes and the top-level process, however, are fully generated using translation rules that make them unique for each Noise Handshake Pattern.

Each handshake message and transport message is given its own `WriteMessage` and `ReadMessage` construction represented as `letfuns` in ProVerif. These functions are constructed to invoke the appropriate state transition functions depending on the tokens included in the message pattern being translated. Consider for example Fig. 5, which concerns the first message in `IK` (Fig. 1): $\rightarrow e, es, s, ss$.

The state transition rules described in §2 are implicated by the tokens within the message pattern. By following these rules, Noise Explorer generates a symbolic model that implements the state transitions relevant to this particular message pattern. From the initiator's side:

- **e**: Signals that the initiator is sending a fresh ephemeral key share as part of this message. This token adds one state transformation to `writeMessage_a`: `mixHash`, which hashes the new key into the session hash.
- **es**: Signals that the initiator is calculating a Diffie-Hellman shared secret derived from the initiator's ephemeral key and the responder's static key as part of this message. This token adds one state transformation to `writeMessage_a`: `mixKey`, which calls the $HKDF$ using as input the existing `SymmetricState` key and $DH(e, rs)$, the Diffie-Hellman share calculated from the initiator's ephemeral key and the responder's static key.

- **`s`**: Signals that the initiator is sending a static key share as part of this message. This token adds one state transformation to `writeMessage_a`: `encryptAndHash` is called on the static public key. If any prior Diffie-Hellman shared secret was established between the sender and the recipient, this allows the initiator to communicate their long-term identity with some degree of confidentiality.
- **`ss`**: Signals that the initiator is calculating a Diffie-Hellman shared secret derived from the initiator's static key and the responder's static key as part of this message. This token adds one state transformation to `writeMessage_a`: `mixKey`, which calls the HKDF function using, as input, the existing `SymmetricState` key, and $DH(s, rs)$, the Diffie-Hellman share calculated from the initiator's static key and the responder's static key.

Message A's payload, which is modeled as the output of the function `msg_a(initiatorIdentity, responderIdentity, sessionId)`, is encrypted as `ciphertext2`. This invokes `encryptAndHash`, which performs AEAD encryption on the payload, with the session hash as the added data (`encryptWithAd`) and `mixHash`, which hashes the encrypted payload into the next session hash.

On the receiver end:

- **`e`**: Signals that the responder is receiving a fresh ephemeral key share as part of this message. This token adds one state transformation to `readMessage_a`: `mixHash`, which hashes the new key into the session hash.
- **`es`**: Signals that the responder is calculating a Diffie-Hellman shared secret derived from the initiator's ephemeral key and the responder's static key as part of this message. This token adds one state transformation to `readMessage_a`: `mixKey`, which calls the HKDF function using, as input, the existing SymmetricState key, and $DH(e, rs)$, the Diffie-Hellman share calculated from the initiator's ephemeral key and the responder's static key.
- **`s`**: Signals that the responder is receiving a static key share as part of this message. This token adds one state transformation to `readMessage_a`: `encryptAndHash` is called on the static public key. If any prior Diffie-Hellman shared secret was established between the sender and the recipient, this allows the initiator to communicate their long-term identity with some degree of confidentiality.
- **`ss`**: Signals that the responder is calculating a Diffie-Hellman shared secret derived from the initiator's static key and the responder's static key as part of this message. This token adds one state transformation to `readMessage_a`: `mixKey`, which calls $HKDF$ function using, as input, the existing `SymmetricState` key and $DH(s, rs)$, the Diffie-Hellman share calculated from the initiator's static key and the responder's static key.

Message A's payload invokes the following operation: `decryptAndHash`, which performs AEAD decryption on the payload, with the session hash as the added data (`decryptWithAd`) and `mixHash`, which hashes the encrypted payload into the next session hash.

4 Modeling Noise Security Guarantees in the Symbolic Model

As described in §2, we consider four "authentication" grades and five "confidentiality" grades when evaluating the security properties of individual messages within Noise Handshake Patterns. In ProVerif, we want to formulate these grades as event-based queries. This implies specifying a number of events triggered at specific points in the protocol flow as well as queries predicated on these events.

4.1 Events

The following events appear in generated ProVerif models:

Syntax

k ::=	public DH keys
e	ephemeral DH key
s	static DH key
t ::=	tokens
k	public DH key
k_1k_2	shared DH secret (ee, es, se, or ss)
psk	pre-shared key
p ::=	pre-messages
ϵ	end of pre-message (empty)
k, p	pre-message with public DH key
m ::=	messages
ϵ	end of message (empty)
t, m	message with token
h_r ::=	handshake (responder's turn)
ϵ	end of handshake
$\xleftarrow{m}\ h_i$	responder message, then initiator's turn
h_i ::=	handshake (initator's turn)
ϵ	end of handshake
$\xrightarrow{m}\ h_r$	initiator message, then responder's turn
n ::=	noise patterns
$\xrightarrow{p_1} \xleftarrow{p_2}\ h_i$	pre-messages, then handshake

Figure 6: Noise Pattern Syntax.

- **`SendMsg(principal, principal, stage, bitstring)`** takes in the identifier of the messager sender, the identifier of the recipient, a "stage" value and the plaintext of the message payload. The "stage" value is the output of a function parametrized by the session ID, a unique value generated for each execution of the protocol using ProVerif's `new` keyword, and an identifier of which message this is within the Noise Handshake Pattern (first message, second message, etc.)
- **`RecvMsg(principal, principal, stage, bitstring)`** is a mirror event of the above, with the first principal referring to the recipient and the second referring to the sender.
- **`LeakS(phasen, principal)`** indicates the leakage of the long-term secret key of the principal. `phasen` refers to which "phase" the leak occured: in generated ProVerif models, phase 0 encompasses protocol executions that occur while the session is under way, while phase 1 is strictly limited to events that occur after the session has completed and has been closed.
- **`LeakPsk(phasen, principal, principal)`** indicates the leakage of the pre-shared key (PSK) of the session between an initiator (specified as the first principal) and a responder in the specified phase.

4.2 Queries

In all examples below, Bob is the sender and Alice is the recipient. The message in question is message D, i.e. the fourth message pattern within the Noise Handshake Pattern. sid_a and sid_b refer to the session ID as registered in the trigger events by Alice and Bob. In valid contexts, these would be the same session ID. A principal c refers to any arbitrary principal on the network, which includes compromised principal Charlie.

In the event of a non-existent static key for either Alice or Bob, or of a non-existent PSK, the relevant `LeakS` or `LeakPsk` event is removed from the query.

4.2.1 Authentication Grade 1

In this query, we test for sender authentication and message integrity. If Alice receives a valid message from Bob, then Bob must have sent that message to someone, or Bob had their static key compromised before the session began, or Alice had their static key compromised before the session began:

$$\begin{aligned}&RecvMsg(alice, bob, stage(d, sid_a), m) \longrightarrow\\&SendMsg(bob, c, stage(d, sid_b), m) \vee\\&(LeakS(phase_0, bob) \wedge LeakPsk(phase_0, alice, bob)) \vee\\&(LeakS(phase_0, alice) \wedge LeakPsk(phase_0, alice, bob))\end{aligned}$$

4.2.2 Authentication Grade 2

In this query, we test for sender authentication and is Key Compromise Impersonation resistance. If Alice receives a valid message from Bob, then Bob must have sent that message to someone, or Bob had their static key compromised before the session began.

$$\begin{aligned}&RecvMsg(alice, bob, stage(d, sid_a), m) \longrightarrow\\&SendMsg(bob, c, stage(d, sid_b), m) \vee\\&LeakS(phase_0, bob)\end{aligned}$$

4.2.3 Authentication Grade 3

In this query, we test for sender and receiver authentication and message integrity. If Alice receives a valid message from Bob, then Bob must have sent that message to Alice specifically, or Bob had their static key compromised before the session began, or Alice had their static key compromised before the session began.

$$\begin{aligned}&RecvMsg(alice, bob, stage(d, sid_a), m) \longrightarrow\\&SendMsg(bob, alice, stage(d, sid_b), m) \vee\\&(LeakS(phase_0, bob) \wedge LeakPsk(phase_0, alice, bob)) \vee\\&(leakS(phase_0, alice) \wedge LeakPsk(phase_0, alice, bob))\end{aligned}$$

4.2.4 Authentication Grade 4

In this query, we test for sender and receiver authentication and is Key Compromise Impersonation resistance. If Alice receives a valid message from Bob, then Bob must have sent that message to Alice specifically, or Bob had their static key compromised before the session began.

$$\begin{aligned}&RecvMsg(alice, bob, stage(d, sid_a), m) \longrightarrow\\&SendMsg(bob, alice, stage(d, sid_b), m) \vee\\&LeakS(phase_0, bob)\end{aligned}$$

4.2.5 Confidentiality Grades 1 and 2

In these query, we test for message secrecy by checking if a passive attacker (for grade 1) or active attacker (for grade 2) is able to retrieve the payload plaintext only by compromising Alice's static key either before or after the protocol session.

$$\begin{aligned}&attacker_{p1}(msg_d(bob, alice, sid_b)) \longrightarrow\\&(LeakS(phase_0, alice) \ \vee\ LeakS(phase_1, alice)) \wedge\\&(LeakPsk(phase_0, alice, bob) \vee\\&LeakPsk(phase_1, alice, bob))\end{aligned}$$

In the above, $attacker_{p1}$ indicates that the attacker is operating in phase 1 of the protocol execution.

Pattern	Auth.	Conf.	Pattern	Auth.	Conf.	Pattern	Auth.	Conf.
N	0	2	X1N	0 0 0 0 2	0 1 1 3 1	I1K1	0 4 4 4 4	0 1 5 5 5
K	1	2	X1K	0 2 0 4 4 4	2 1 5 3 5 5	I1X	0 4 4 4 4	0 1 5 5 5
X	1	2	XK1	0 2 4 4 4	0 1 5 5 5	IX1	0 0 4 4 4	0 3 3 5 5
NN	0 0 0	0 1 1	X1K1	0 2 0 4 4 4	0 1 5 3 5 5	I1X1	0 0 4 4 4	0 1 3 5 5
NK	0 2 0	2 1 5	X1X	0 2 0 2 2 2	0 1 5 3 5 5	Npsk0	1	2
NX	0 2 0	0 1 5	XX1	0 0 4 4 4	0 1 3 5 5	Kpsk0	1	2
XN	0 0 2 0	0 1 1 5	X1X1	0 0 0 4 4 4	0 1 3 3 5 5	Xpsk1	1	2
XK	0 2 4 4 4	2 1 5 5 5	K1N	0 0 2 0	0 1 1 5	NNpsk0	1 1 1 1	2 3 3 3
XX	0 2 4 4 4	0 1 5 5 5	K1K	0 4 4 4 4	2 1 5 5 5	NNpsk2	0 1 1 1	0 3 3 3
KN	0 0 2 0	0 3 1 5	KK1	0 4 4 4	0 3 5 5	NKpsk0	1 4 1 4	2 5 3 5
KK	1 4 4 4	2 4 5 5	K1K1	0 4 4 4	0 1 5 5 5	NKpsk2	0 4 1 4	0 3 3 5
KX	0 4 4 4	0 3 5 5	K1X	0 4 4 4 4	0 1 5 5 5	NXpsk2	0 4 1 4	0 3 3 5
IN	0 0 2 0	0 3 1 5	KX1	0 0 4 4 4	0 3 3 5 5	XNpsk3	0 0 4 1 4	0 1 3 3 5
IK	1 4 4 4	2 4 5 5	K1X1	0 0 4 4 4	0 1 3 5 5	XKpsk3	0 0 4 4 4	0 1 3 5 5
IX	0 4 4 4	0 3 5 5	I1N	0 0 2 0 2	0 1 1 5 1	KNpsk0	1 1 4 1	2 3 5 3
NK1	0 2 0	0 1 5	I1K	0 4 4 4 4	2 1 5 5 5	KNpsk2	0 1 4 1	0 3 5 3
NX1	0 0 0 2 0	0 1 3 1 5	IK1	0 4 4 4	0 3 5 5	INpsk1	1 1 4 1	2 3 5 3

Figure 7: Verification results for 50 Noise Handshake Patterns.

4.2.6 Confidentiality Grades 3 and 4

In this query, we test for forward secrecy by checking if a passive attacker is able to retrieve the payload plaintext only by compromising Alice's static key before the protocol session, or after the protocol session along with Bob's static public key (at any time.)

$$\begin{aligned}
&attacker_{p1}(msg_d(bob, alice, sid_b)) \longrightarrow \\
&(LeakS(phase_0, alice)\ \wedge\ LeakPsk(phase_0, alice, bob)) \vee \\
&(LeakS(p_x, alice)\ \wedge\ LeakPsk(p_y, alice, bob) \wedge \\
&LeakS(p_z, bob))
\end{aligned}$$

In the above, p_x, p_y, p_z refer to any arbitrary phases.

4.2.7 Confidentiality Grade 5

In this query, we test for strong forward secrecy by checking if an active attacker is able to retrieve the payload plaintext only by compromising Alice's static key before the protocol session.

$$\begin{aligned}
&attacker_{p1}(msg_d(bob, alice, sid_b)) \longrightarrow \\
&(LeakS(phase_0, alice) \wedge LeakPsk(phase_0, alice, bob))
\end{aligned}$$

A set of the above queries is generated for each handshake and transport message within a Noise Handshake Pattern, allowing for verification to occur in the comprehensive context described in §3. Whenever a pattern contains a PSK and `LeakPSK` events start to get involved, we ideally account for cases where one long-term secret is compromised but not the other. This indicates that we may need a richer notion of authenticity and confidentiality grades than the 1-5 markers that the Noise specification provides. For consistency, we are still using the old grades, but to truly understand and differentiate the security provided in many cases, we recommend that the user view the detailed queries and results as generated by Noise Explorer and available in its detailed rendering of the verification results.

5 Reasoning About Noise Handshake Patterns with Noise Explorer

A central motivation to this work is the obtention of a general framework for designing, reasoning about, formally verifying and comparing any arbitrary Noise Handshake Pattern. Noise Explorer is a web framework that implements all of the formalisms and ProVerif translation logic described so far in this work in order to provide these features.

Noise Explorer is ready for use by the general public today at `https://noiseexplorer.com`. Here are Noise Explorer's main functionalities:

Designing and validating Noise Handshake Patterns. This allows protocol designers to immediately obtain validity checks that verify if the protocol conforms to the latest Noise Protocol Framework specification.[7]

Generating cryptographic models for formal verification using automated verification tools. Noise Explorer can compile any Noise Handshake Pattern to a full representation in the applied-pi calculus including cryptographic primitives, state machine transitions, message passing and a top-level process illustrating live protocol execution. Using ProVerif, we can then test against sophisticated security queries starting at basic confidentiality and authentication and extending towards forward secrecy, post-compromise security and resistance to key compromise impersonation. The models can also be used as a foundation for further modeling using the CryptoVerif [19] computational model protocol prover.

Exploring the first compendium of formal verification results for Noise Handshake Patterns. Since formal verification for complex Noise Handshake Patterns can take time and require fast CPU hardware, Noise Explorer comes with a compendium detailing the full results of all Noise Handshake Patterns described in the latest revision of the original Noise Protocol Framework specification. These results are presented with a security model that is even more comprehensive than the original specification, as described in §4.

5.1 Accessible High Assurance Verification for Noise-Based Protocols

Noise Explorer users are free to specify any arbitrary Noise Handshake Pattern of their own design. Once this input is validated, formal verification models are generated. the ProVerif verification output can then be fed right back into Noise Explorer, which will then generate detailed interactive pages describing the analysis results.

The initial view of the results includes a pedagogical plain-English paragraph for each message summarizing its achieved security guarantees. For example, the following paragraph is generated for message D of `IK`:

*"Message D, sent by the responder, benefits from **sender and receiver authentication** and is **resistant to Key Compromise Impersonation**. Assuming the corresponding private keys are secure, this authentication cannot be forged. Message contents benefit from **message secrecy** and **strong forward secrecy**: if the ephemeral private keys are secure and the initiator is not being actively impersonated by an active attacker, message contents cannot be decrypted."*

Furthermore, each message comes with a detailed analysis view that allows the user to immediately access a dynamically generated representation of the state transition functions for this particular message as modeled in ProVerif and a more detailed individual writeup of which security goals are met and why. We believe that this *"pedagogy-in-depth"* that is provided by the Noise Explorer web framework will allow for useful, push-buttom analysis of any constructed protocol within the Noise Protocol Framework that is highly comprehensive.

Noise Explorer's development was done in tandem with discussions with the Noise Protocol Framework author: pre-release versions were built around revision 33 of the Noise Protocol Framework and an update to support revision 34 of the framework was released in tandem with the specification revision draft. Revision 34 also included security grade results for deferred patterns that were obtained

[7]As of writing, Revision 34 is the latest draft of the Noise Protocol Framework. Noise Explorer is continuously updated in collaboration with the authors of the Noise Protocol Framework specification.

directly via Noise Explorer's compendium of formal analysis results. We plan to continue collaborating with the Noise Protocol Framework author indefinitely to support future revisions of the Noise Protocol Framework.

5.2 Modeling for Forgery Attacks in Noise Explorer

Using ProVerif, we were able to test for and discover a novel forgery attack within certain Noise Handshake Patterns. Essentially, we can compose well-known attack vectors (invalid Diffie-Hellman key shares, repeated AEAD nonces) to attack patterns that rely only on static-static key derivation (`ss`) for authentication.

As we explain later in this section, the pattern underlying this finding is not considered as valid in the latest version of the Noise Protocol Framework specification and its validity was already ambiguous, if not outright disallowed, in previous revisions.

Consider the pattern `KXS` below:

$$\begin{aligned} KXS:&\\ &\rightarrow s\\ &\dots\\ &\rightarrow e\\ &\leftarrow e, ee, s, ss \end{aligned}$$

This is a variation of the Noise Handshake Pattern `KX` that uses `ss` instead of `se`, and `es`, so it is a little more efficient while satisfying the same confidentiality and authentication goals. In particular, the responder can start sending messages immediately after the second message.

However, there is an attack if the responder does not validate ephemeral public values. Suppose a malicious initiator were to send an invalid ephemeral public key `e`, say $e = 0$. Then, because of how Diffie-Hellman operations work on X25519, the responder would compute $ee = 0$ and the resulting key would depend only on the static key `ss`. Note that while the responder could detect and reject the invalid public key, the Noise specification explicitly discourages this behavior.

Since the responder will encrypt messages with a key determined only by `ss` (with a nonce set to 0), the malicious initiator can cause it to encrypt two messages with the same key and nonce, which allows for forgery attacks. A concrete man-in-the-middle attack on this pattern is as follows:[8]

In the pre-message phase, A sends a public static key share s_A to B. In the first session:

1. A malicious C initiates a session with B where he pretends to be A. C sends $e = Z$ such that Z^x would evaluate to Z for any x. This effectively allows us to model for forcing an X25519 zero-value key share in the symbolic model.

2. B receives $e = Z$ and accepts a new session with:
   - $h_{B0} = H(\texttt{pattern\_name})$
   - $ck_{B1} = h_{B0}$
   - $h_{B1} = H(h_{B0}, s_A, e = Z)$

3. B generates re_1, computes $ee = Z$ and sends back $(re_1, ee = Z, s_B, ss_{AB}, msg_a)$ where s_B is encrypted with $ck_{B2} = H(ck_{B1}, ee = Z)$ as the key, 0 as the nonce and $h_{B2} = H(h_{B1}, re_1, ee = Z)$ as additional data.

4. msg_a is encrypted with $ck_{B3} = H(ck_{B2}, ss_{AB})$ as the key, 0 as the nonce and $h_{B3} = H(h_{B2}, s_B)$ as additional data.

5. C discards this session but remembers the encrypted message.

[8]For simplicity, here we use H to represent the more complex key derivation and mixing functions.

In a second session:

1. A initiates a session with B by sending e. So, at A:
   - $h_{A0} = H(\texttt{pattern\_name})$
   - $ck_{A1} = h_{A0}$
   - $h_{A1} = H(h_{A0}, s_A, e)$
2. C intercepts this message and replaces it with the invalid public key $Z = 0$.
3. B receives $e = Z$ and accepts a new session with:
   - $h_{B0} = H(\texttt{pattern\_name})$
   - $ck_{B1} = h_{B0}$
   - $h_{B1} = H(h_{B0}, s_A, e = Z)$
4. B generates re_2, computes $ee = Z$ and sends back $(re_2, ee = Z, s_B, ss_{AB}, msg_b)$ where s_B is encrypted with $ck_{B2} = H(ck_{B1}, ee = Z)$ as the key, 0 as the nonce and $h_{B2} = H(h_{B1}, re)$ as additional data.
5. msg_b is encrypted with $ck_{B3} = H(ck_{B2}, ss_{AB})$ as the key, 0 as the nonce and $h_{B3} = H(h_{B2}, s_B)$ as additional data.
6. C intercepts this response.

Notably, the encryption keys (ck_{B3}) and the nonces (0) used for msg_a in session 1 and msg_b in session 2 are the same. Hence, if the underlying AEAD scheme is vulnerable to the repeated nonces attack, C can compute the AEAD authentication key for ck_{B3} and tamper with msg_a and msg_b to produce a new message msg_c that is validly encrypted under this key. Importantly, C can also tamper with the additional data h_{B3} to make it match any other hash value.

C replaces the message with $(re = Z, ee = Z, s_B, ss_{AB}, msg_c)$ and sends it to A, where s_B is re-encrypted by C using ck_{B2} which it knows and msg_c is forged by C using the AEAD authentication key for ck_{B3}. A receives the message $(re = Z, ee = Z, s_B, ss_{AB}, msg_c)$ and computes $ck_{A2} = H(ck_{A1}, ee = Z)$ and $h_{A2} = H(h_{A1}, ee = Z)$. A then decrypts s_B. A then computes $ck_{A3} = H(ck_{A2}, ss_{AB})$ and $h_{A3} = H(h_{A2}, s_{AB})$ and decrypts msg_c. This decryption succeeds since $ck_{A3} = ck_{B3}$. The attacker C therefore has successfully forged the message and the added data. At a high level, the above analysis can be read as indicating one of three shortcomings:

1. **Using `ss` in Noise Handshake Patterns must be done carefully.** A Noise Handshake Pattern validation rule could be introduced to disallow the usage of `ss` in a handshake unless it is accompanied by `se` or `es` in the same handshake pattern.
2. **Diffie-Hellman key shares must be validated.** Implementations must validate incoming Diffie-Hellman public values to check that they are not one of the twelve known integers which can cause a scalar multiplication on the X25519 curve to produce an output of 0.
3. **Independent sessions must be checked for AEAD key reuse.** Ephemeral and static public key values are mixed into the encryption key derivation step.

The attack described above was reported to the Noise Protocol Framework author. The author's response revolved around the fact that `KXS` was only considered a valid Noise Protocol Framework pattern due to a lack of clarity in the then-current revision of the specification. As a result of our report, revision 34 of the Noise Protocol Framework specification included the following more stringent pattern validity rule:

After calculating a Diffie-Hellman shared secret between a remote public key (either static or ephemeral) and the local static key, the local party must not perform any encryptions unless it has also calculated a Diffie-Hellman key share between its local ephemeral key and the remote public key. In particular, this means that:

- After an `se` or `ss` token, the initiator must not send a payload unless there has also been an `ee` or `es` token respectively.
- After an `es` or `ss` token, the responder must not send a payload unless there has also been an `ee` or `se` token respectively.

These new validity rules were implemented into Noise Explorer's pattern validation logic.

6 Discussion and Future Work

In this work, we have provided the first formal treatment of the Noise Protocol Framework. We translate our formalisms into the applied-pi calculus and use this as the basis for automatically generating models for the automated formal verification of arbitrary Noise Handshake Patterns. We coalesce our results into Noise Explorer, an online framework for pedagogically designing, validating, verifying and reasoning about arbitrary Noise Handshake Patterns.

Noise Explorer has already had an impact as the first automated formal analysis targeting any and all Noise Handshake Patterns. Verification results obtained from Noise Explorer were integrated into the original specification and precisions were made to the validation rules and security goals as a result of the scrutiny inherent to our analysis.

Ultimately, it is not up to us to comment on whether Noise presents a "good" framework, per se. However, we present confident results that its approach to protocol design allows us to cross a new bridge for not only designing and implementing more robust custom secure channel protocols, but also applying existing automated verification methodologies in new and more ambitious ways.

Future work could include the automated generation of computational models to be verified using CryptoVerif and of verified implementations of Noise Handshake Patterns. The scope of our formalisms could also be extended to include elements of the Noise Protocol Framework specification, such as queries to test for identity hiding.

Acknowledgements

We would like to thank Bruno Blanchet for his insight with regards to modeling and optimization in ProVerif.

References

[1] Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Alfredo Pironti, and Pierre-Yves Strub. Triple handshakes and cookie cutters: Breaking and fixing authentication over TLS. In *IEEE Symposium on Security & Privacy (Oakland)*, pages 98–113, 2014.

[2] Gavin Lowe. An attack on the needham- schroeder public- key authentication protocol. *Information processing letters*, 56(3), 1995.

[3] Roger M Needham and Michael D Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12):993–999, 1978.

[4] Karthikeyan Bhargavan, Antoine Delignat-Lavaud, and Alfredo Pironti. Verified contributive channel bindings for compound authentication. In *Network and Distributed System Security Symposium (NDSS '15)*, 2015.

[5] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, et al. Imperfect forward secrecy: How Diffie-Hellman fails in practice. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 5–17, 2015.

[6] Trevor Perrin. The Noise protocol framework, 2015. Available at `http://www.noiseprotocol.org`.

[7] Vincent Cheval and Bruno Blanchet. Proving more observational equivalences with ProVerif. In *International Conference on Principles of Security and Trust*, pages 226–246. Springer, 2013.

[8] Bruno Blanchet. Modeling and verifying security protocols with the applied pi calculus and ProVerif. *Foundations and Trends in Privacy and Security*, 1(1–2):1–135, October 2016.

[9] Martín Abadi, Bruno Blanchet, and Cédric Fournet. The applied pi calculus: Mobile values, new names, and secure communication. *J. ACM*, 65(1):1:1–1:41, 2018.

[10] Jason A Donenfeld. WireGuard: next generation kernel network tunnel. In *24th Annual Network and Distributed System Security Symposium, NDSS*, 2017.

[11] Benjamin Lipp. A Mechanised Computational Analysis of the WireGuard Virtual Private Network Protocol.

[12] Jason Donenfeld and Kevin Milner. Formal verification of the wireguard protocol, 2017. https://www.wireguard.com/formal-verification/.

[13] Benjamin Dowling and Kenneth G. Paterson. A cryptographic analysis of the wireguard protocol. Cryptology ePrint Archive, Report 2018/080, 2018. `https://eprint.iacr.org/2018/080`.

[14] N. Kobeissi, K. Bhargavan, and B. Blanchet. Automated verification for secure messaging protocols and their implementations: A symbolic and computational approach. In *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2017.

[15] Karthikeyan Bhargavan, Bruno Blanchet, and Nadim Kobeissi. Verified models and reference implementations for the tls 1.3 standard candidate. In *Security and Privacy (SP), 2017 IEEE Symposium on*, pages 483–502. IEEE, 2017.

[16] Phillip Rogaway. Authenticated-encryption with associated-data. In *Ninth ACM Conference on Computer and Communications Security (CCS-9)*, pages 98–107, Washington, DC, November 2002. ACM Press.

[17] H. Krawczyk. Cryptographic extraction and key derivation: The HKDF scheme. In *Advances in Cryptology (CRYPTO)*, pages 631–648. 2010.

ProVerif

$M ::=$	terms
v	values
a	names
$f(M_1, \ldots, M_n)$	function application
$E ::=$	enriched terms
M	return value
$\texttt{new}\ a : \tau; E$	new name a of type τ
$\texttt{let}\ x = M\ \texttt{in}\ E$	variable definition
$\texttt{if}\ M = N\ \texttt{then}\ E_1\ \texttt{else}\ E_2$	if-then-else
$P, Q ::=$	processes
0	null process
$\texttt{in}(M, x : \tau); P$	input x from channel M
$\texttt{out}(M, N); P$	output N on channel M
$\texttt{let}\ x = M\ \texttt{in}\ P$	variable definition
$P \mid Q$	parallel composition
$!P$	replication of P
$\texttt{insert}\ a(M_1, \ldots, M_n); P$	insert into table a
$\texttt{get}\ a(=M_1, x_2, \ldots, x_n)\ \texttt{in}\ P$	get table entry specified by M_1
$\texttt{event}\ M; P$	event M
$\texttt{phase}\ n; P$	enter phase n
$\Delta ::=$	declaration
$\texttt{type}\ \tau$	type τ
$\texttt{free}\ a : \tau$	name a
$\texttt{query}\ q$	query q
$\texttt{table}\ a(\tau_1, \ldots, \tau_n)$	table a
$\texttt{fun}\ C(\tau_1, \ldots, \tau_n) : \tau$	constructor
$\texttt{reduc}\ \texttt{forall}\ x_1 : \tau_1, \ldots, x_n : \tau_n; f(M_1, \ldots, M_n) = M$	destructor
$\texttt{equation}\ \texttt{forall}\ x_1 : \tau_1, \ldots, x_n : \tau_n; M = M'$	equation
$\texttt{letfun}\ f(x_1 : \tau_1, \ldots, x_n : \tau_n) = E$	pure function
$\texttt{let}\ p(x_1 : \tau_1, \ldots, x_n : \tau_n) = P$	process
$\Sigma ::= \Delta_1. \ldots \Delta_n.\texttt{process}\ P$	script

Figure 8: ProVerif syntax, based on the applied-pi calculus.

[18] Daniel J. Bernstein. Curve25519: New Diffie-Hellman speed records. In *Public Key Cryptography (PKC)*, pages 207–228, 2006.

[19] Bruno Blanchet. CryptoVerif: Computationally sound mechanized prover for cryptographic protocols. In *Dagstuhl seminar "Formal Protocol Verification Applied*, page 117, 2007.

```
let initiator(me:principal, them:principal, sid:sessionid) =
let s = keypairpack(bit2key(empty), bit2key(empty)) in
out(pub, getpublickey(s));
((let e = keypairpack(bit2key(empty), bit2key(empty)) in
    let rs = getpublickey(generate_keypair(key_s(them))) in
    let re = bit2key(empty) in
    let hs:handshakestate = initialize_initiator(empty, s, e, rs, re, bit2key(empty)) in
    insert statestore(me, them, sid, statepack_a(hs))
) | (get statestore(=me, =them, =sid, statepack_a(hs)) in
    let (hs:handshakestate, message_a: bitstring) = writeMessage_a(me, them, hs, msg_a(me, them, sid), sid) in
    event SendMsg(me, them, stagepack_a(sid), msg_a(me, them, sid));
    insert statestore(me, them, sid, statepack_b(hs));
    out(pub, message_a)
) | (get statestore(=me, =them, =sid, statepack_b(hs)) in
    in(pub, message_b:bitstring);
    let (hs:handshakestate, plaintext_b: bitstring, valid:bool, cs1: cipherstate, cs2:cipherstate) = readMessage_b(me, them, hs, message_b, sid) in
    event RecvMsg(me, them, stagepack_b(sid), plaintext_b);
    insert statestore(me, them, sid, statepack_c(hs, cs1, cs2));
    0
) | !(get statestore(=me, =them, =sid, statepack_c(hs, cs1, cs2)) in
    let hs = handshakestatesetcs(hs, cs1) in
    let (hs:handshakestate, message_c: bitstring) = writeMessage_c(me, them, hs, msg_c(me, them, sid), sid) in
    event SendMsg(me, them, stagepack_c(sid), msg_c(me, them, sid));
    insert statestore(me, them, sid, statepack_d(hs, handshakestategetcs(hs), cs2));
    out(pub, message_c)
) | !(get statestore(=me, =them, =sid, statepack_d(hs, cs1, cs2)) in
    let hs = handshakestatesetcs(hs, cs2) in
    in(pub, message_d:bitstring);
    let (hs:handshakestate, plaintext_d: bitstring, valid:bool) = readMessage_d(me, them, hs, message_d, sid) in
    event RecvMsg(me, them, stagepack_d(sid), plaintext_d);
    (* Final message, do not pack state *)
    event RecvEnd(valid)
) | (event LeakS(phase0, me);
    out(pub, key_s(me))
) | (phase 1;
    event LeakS(phase1, me);
    out(pub, key_s(me)))).
```

```
let responder(me:principal, them:principal, sid:sessionid) =
let s = generate_keypair(key_s(me)) in
out(pub, getpublickey(s));
((let e = keypairpack(bit2key(empty), bit2key(empty)) in
    let rs = bit2key(empty) in
    let re = bit2key(empty) in
    let hs:handshakestate = initialize_responder(empty, s, e, rs, re, bit2key(empty)) in
    insert statestore(me, them, sid, statepack_a(hs))
) | (get statestore(=me, =them, =sid, statepack_a(hs)) in
    in(pub, message_a:bitstring);
    let (hs:handshakestate, plaintext_a: bitstring, valid:bool) = readMessage_a(me, them, hs, message_a, sid) in
    event RecvMsg(me, them, stagepack_a(sid), plaintext_a);
    insert statestore(me, them, sid, statepack_b(hs));
    0
) | (get statestore(=me, =them, =sid, statepack_b(hs)) in
    let (hs:handshakestate, message_b: bitstring, cs1:cipherstate, cs2: cipherstate) = writeMessage_b(me, them, hs, msg_b(me, them, sid), sid) in
    event SendMsg(me, them, stagepack_b(sid), msg_b(me, them, sid));
    insert statestore(me, them, sid, statepack_c(hs, cs1, cs2));
    out(pub, message_b)
) | !(get statestore(=me, =them, =sid, statepack_c(hs, cs1, cs2)) in
    let hs = handshakestatesetcs(hs, cs1) in
    in(pub, message_c:bitstring);
    let (hs:handshakestate, plaintext_c: bitstring, valid:bool) = readMessage_c(me, them, hs, message_c, sid) in
    event RecvMsg(me, them, stagepack_c(sid), plaintext_c);
    insert statestore(me, them, sid, statepack_d(hs, handshakestategetcs(hs), cs2));
    0
) | !(get statestore(=me, =them, =sid, statepack_d(hs, cs1, cs2)) in
    let hs = handshakestatesetcs(hs, cs2) in
    let (hs:handshakestate, message_d: bitstring) = writeMessage_d(me, them, hs, msg_d(me, them, sid), sid) in
    event SendMsg(me, them, stagepack_d(sid), msg_d(me, them, sid));
    (* Final message, do not pack state *)
    out(pub, message_d)
) | (event LeakS(phase0, me);
    out(pub, key_s(me))
) | (phase 1;
    event LeakS(phase1, me);
    out(pub, key_s(me)))).
```

Figure 9: Initiator and responder processes for the `IK` Noise Handshake Pattern.