A Spectral Analysis of Noise: A Comprehensive, Automated, Formal Analysis of Diffie-Hellman Protocols

Guillaume Girol[1] Lucca Hirschi[2] Ralf Sasse[3] Dennis Jackson[4] Cas Cremers[5] David Basin[3]

[1]CEA, List, Université Paris-Saclay, France

[2]Inria & LORIA, France

[3]Department of Computer Science, ETH Zurich

[4]University of Oxford, United Kingdom

[5]CISPA Helmholtz Center for Information Security

The Noise family or protocols

Noise:

- secure channel between Alice and Bob
- based on Diffie-Hellman key exchange

The Noise family or protocols

Noise:

- secure channel between Alice and Bob
- based on Diffie-Hellman key exchange

Noise is a large family (technically infinite)

Ex: Wireguard, Lightning, Whatsapp use 3 distinct Noise protocols

Meant to adapt to many use cases:

	Alice	Bob
Has long-term key	**Yes/No**	**Yes/No**
Knows peer's long-term key	**Yes/No**	**Yes/No**
Shared symmetric key material	**Yes/No**	
...		

Choosing a Noise protocol

In the Noise specification: 50+ examples with widely different security guarantees, and you can even build your own!

Our goal

Helping practitioners choose the Noise protocol with the best security guarantees given their requirements and threat model

Manual comparison is impossible → do it automatically with formal methods!

Analysis based on the Tamarin prover:

- symbolic verification
- precise modelling of Diffie-Hellman operations

What we want to know

Proof goals

$$\text{A Noise protocol} + \left\{\begin{array}{l}\text{Secrecy}\\ \text{Agreement}\\ \text{Anonymity*}\end{array}\right. + \text{A threat model} \rightarrow \left\{\begin{array}{c}\text{yes}\\ \text{no}\\ \text{timeout}\end{array}\right.$$

*some limitations

What we want to know

Proof goals

$$\text{A Noise protocol} + \left\{ \begin{array}{l} \text{Secrecy} \\ \text{Agreement} \\ \text{Anonymity*} \end{array} \right. + \text{A threat model} \rightarrow \left\{ \begin{array}{c} \text{yes} \\ \text{no} \\ \text{timeout} \end{array} \right.$$

What threat models?

Any combination (∧,∨) of *adversary capabilities*:

- be active
- impersonate Alice/Bob/the PKI
- compromise keys before the session
- compromise keys at any time

→ more than 10^{12} threat models!

*some limitations

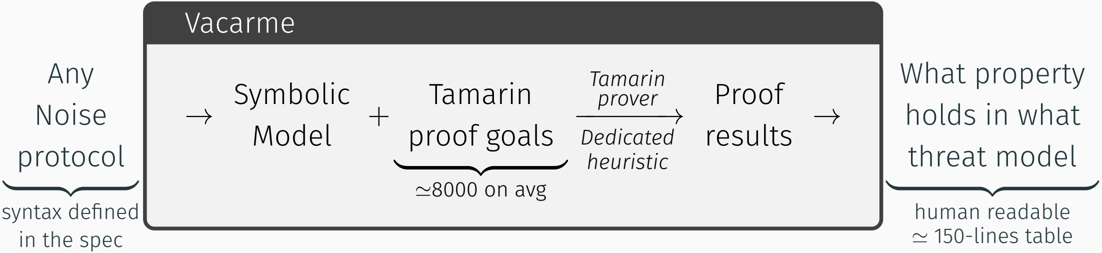
Contribution 1: the *Vacarme* tool

Vacarme automatically derives the security properties of any Noise protocol

Challenge: not enumerating all possible proof goals

using the structure of the problem: some proof goals subsume each other, the ones we prove are soundly, carefully selected

preprocessing: Vacarme includes a light-weight incomplete prover for "easy proofs"



Any Noise protocol

syntax defined in the spec

Vacarme

→ Symbolic Model + Tamarin proof goals

≃8000 on avg

Tamarin prover → *Dedicated heuristic*

Proof results →

What property holds in what threat model

human readable

≃ 150-lines table

Contribution 2: results on the Noise specification

We ran Vacarme on the 53 Noise protocols[†] given as examples in the Noise specification. Gives new insight, *e.g.*

- The Noise specification claims informal *security levels* (secrecy: $0 \to 5$ ...)
    - Prior work (Noise Explorer) proved them
    - We show they hold only if ephemeral keys do not leak
    - Not monotonic: upgrading from level 3 to level 5 can break secrecy
    - Vacarme *procedurally* infers a formal meaning for secrecy & agreement levels
- Session identifiers must remain private (leaks break anonymity)
- Adding a dummy pre-shared key sometimes worsens guarantees

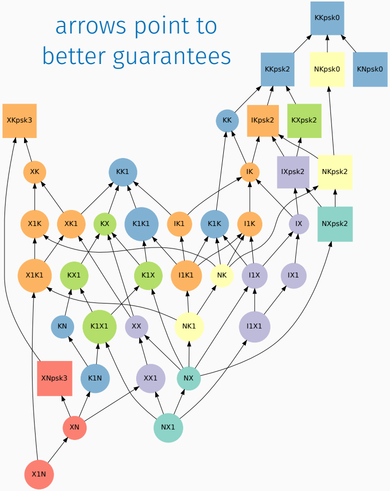
[†] partial results for anonymity

Contribution 3: what Noise protocol should I choose?

A partial order on Noise protocols

A is better than *B* when for any property *p* and threat model *t*, if *p* holds in *t* in protocol *B*, then *p* also holds in *t* in protocol *A*.

Identical properties must be studied in *A* and *B*. Requires special care in the formulation of agreement properties.



arrows point to better guarantees

Contribution 3: what Noise protocol should I choose? Example

Example

If Alice and Bob both have a long-term key and Bob knows Alice's:

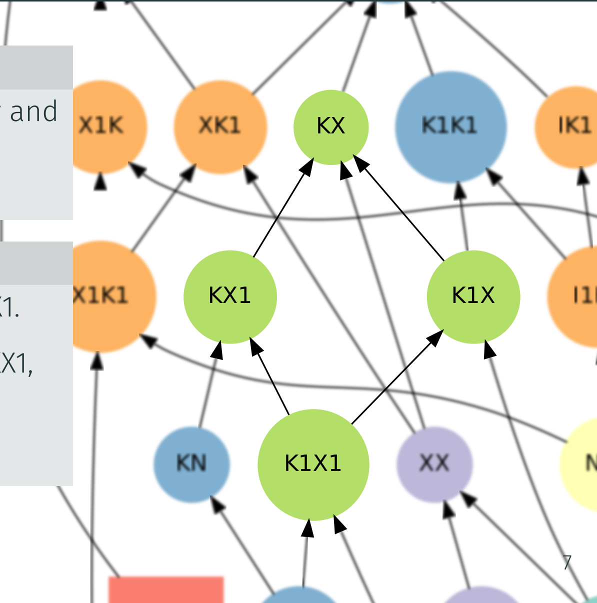
4 candidates: KX, K1X, KX1, K1X1, in green →

Redundant Noise protocols

KX has better guarantees than K1X, KX1, K1X1.

No (cryptographic) reason to choose K1X, KX1, K1X1: they are redundant Noise protocols.

We identify 20 redundant Noise protocols.



Summary

Vacarme: an automated tool to determine the security guarantees of Noise protocols that can compare them to help choose the best ones.

Full results & source code as artifacts to the paper

Thank you for your attention

Contact: `guillaume.girol@cea.fr`