



How to build post-quantum cryptographic protocols and why wall clocks are not to be trusted.

Benjamin Lipp, **Karolin Varner**, and **Lisa Schmidt**  
with support from Alice Bowman, and Marei Peischl  
<https://rosenpass.eu>



## This is the Plan

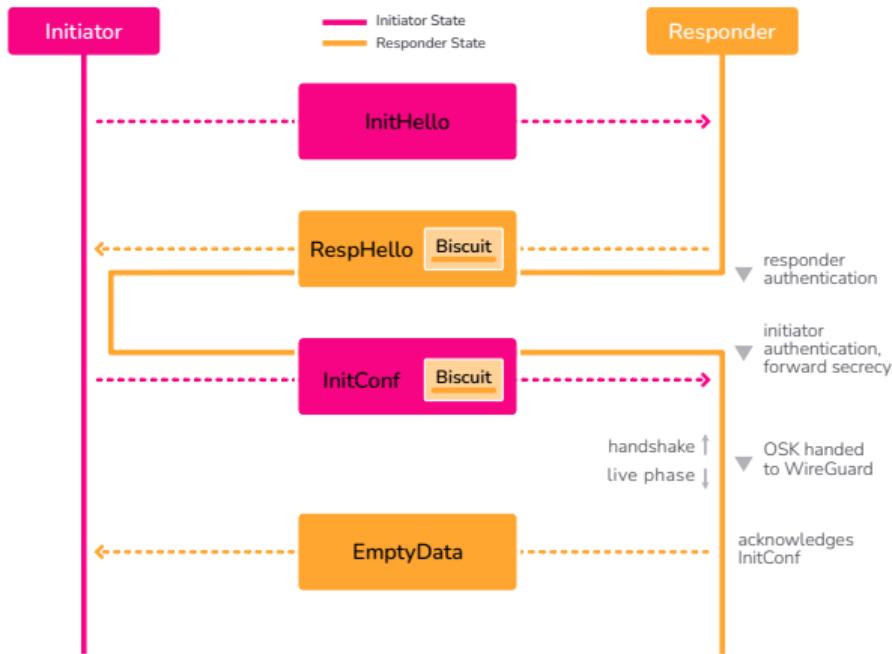
1. **Introducing Rosenpass**, briefly.
2. **The Design of Rosenpass** and basics about post-quantum protocols.
3. **Hybrid Security** – how it can be done and how we do it.
4. **ChronoTrigger Attack** and not trusting wall clocks.
5. **Protocol Proofs** – big old rant!





## Introducing Rosenpass, briefly

- A post-quantum secure key exchange **protocol** based on the paper Post-Quantum WireGuard [PQWG]
- An open-source Rust **implementation** of that protocol, already in use
- A way to secure WireGuard VPN setups against quantum attacks
- A **post-quantum secure VPN**
- A governance **organization** to facilitate development, maintenance, and adoption of said protocol



# The Design of Rosenpass

and how to build post-quantum protocols





In the following slides you will learn ...

... that, to a crypto protocol designer, post-quantum cryptography is not much more than a subtle difference in function interface.



## Glossary: Post-Quantum Security

Pre-quantum  
cryptography is ...

... susceptible to attacks from  
quantum computers.

Post-quantum  
cryptography is ...

... not susceptible to attacks  
from quantum computers.

Hybrid cryptography  
combines ...

... the combination of the  
previous two. It is ...

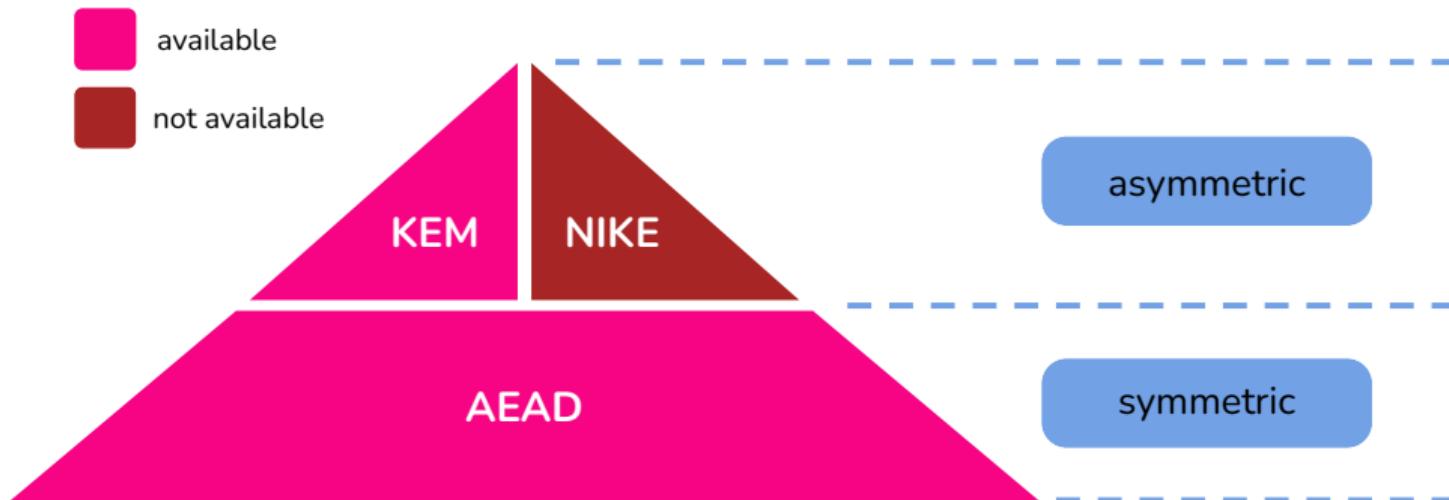
- Specifically, to *Shor's Algorithm*
- Quite fast
- Widely widely trusted

- generally less efficient.
- much bigger ciphertexts.
- less analyzed.

- about as inefficient as post-quantum cryptography.
- not widely adopted, which is a major problem.



## What Post-Quantum Got





## KEMs and NIKEs

### Key Encapsulation Method

```
fn Kem::encaps(Pk) -> (Shk, Ct);
fn Kem::decaps(Pk, Ct) -> Shk;
```

```
(shk, ct) = encaps(pk);
assert!(decaps(sk, ct) = shk)
```

Think of it as encrypting a key and sending it to the partner.

- Secrecy
- Implicit authentication of recipient  
(assuming they have the shared key, they must also have their secret key)

### Non-Interactive Key Exchange

```
fn nike(sk: Sk, pk: Pk) -> Shk;
assert!(nike(sk1, pk2) =
          nike(sk2, pk1));
```

Aka. Diffie-Hellman. I don't know a good analogy, but note how the keypairs are crossing over to each other.

- Secrecy
- Implicit mutual authentication (for each party: assuming they have the shared key, they must also have their secret key)



# Protocol Security Properties

## Implicit authentication

"If you have access to this shared symmetric key then you must have a particular asymmetric secret key."

## Explicit authentication

"I know you have access to this shared key because I checked by making you use it, therefore you also have a particular asymmetric secret key."

## Secrecy

"The data we exchange cannot be decrypted unless someone gets their hands on some of our static keys!"

## Forward secrecy

"Even if our static keys are exposed, the data we exchanged cannot be retroactively decrypted!" \*

\* Terms and conditions apply: We are using an extra key that we do not call a *static* key. This key is generated on the fly, not written to disk and immediately erased after use, so it is more secure than our static keys. Engaging in cryptography is a magical experience but technological constructs can – at best – be asymptotically indistinguishable from miracles.



## KEMs and NIKEs: Key Exchange

### Key Encapsulation Method

**Responder Authentication:** Initiator encapsulates key under the responder public key.

**Initiator Authentication:** Responder encapsulates key under the initiator public key.

**Forward Secrecy:** For the case the secret keys get stolen, either party generates a temporary keypair and has the other party encapsulate a secret under that keypair.

How to do this properly? See Rosenpass.

### Non-Interactive Key Exchange

**Responder Authentication:** Static-static NIKE since NIKE gives mutual authentication.

**Initiator Authentication:** Static-static NIKE since NIKE gives mutual authentication.

**Forward-secrecy:** Another NIKE, involving a temporary keypair.

How to do this properly? See the Noise Protocol Framework.



# KEMs and NIKEs

## Key Encapsulation Method

```

trait Kem {
    // Secret, Public, Symmetric, Ciphertext
    type Sk; type Pk; type Shk; type Ct;
    fn genkey() -> (Sk, Pk);
    fn encaps(pk: Pk) -> (Shk, Ct);
    fn decaps(sk: Pk, ct: Ct) -> Shk;
}
#[test]
fn test<K: Kem>() {
    let (sk, pk) = K::genkey();
    let (shk1, ct) = K::encaps(pk);
    let shk2 = K::decaps(sk, ct);
    assert_eq!(shk1, shk2);
}

```

## Non-Interactive Key Exchange

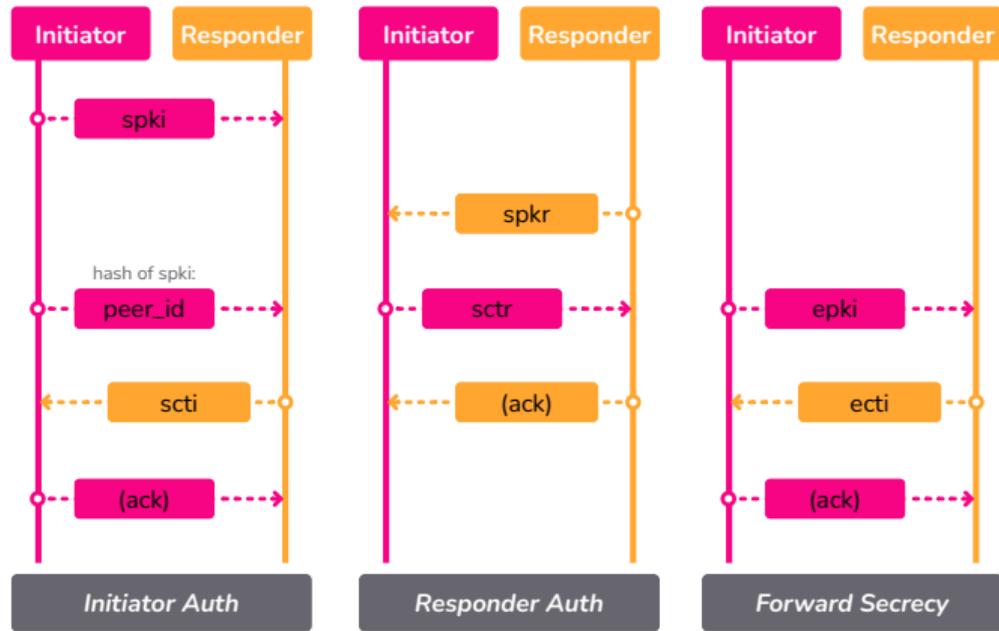
```

trait Nike {
    // Secret, Public, Symmetric
    type Sk; type Pk; type Shk;
    fn genkey() -> (Sk, Pk);
    fn nike(sk: Sk, pk: Pk) -> Shk;
}
#[test]
fn test<N: Nike>() {
    let (sk1, pk1) = N::genkey();
    let (sk2, pk2) = N::genkey();
    let ct1 = N::nike(sk1, pk2);
    let ct2 = N::nike(sk2, pk1);
    assert_eq!(ct1, ct2);
}

```

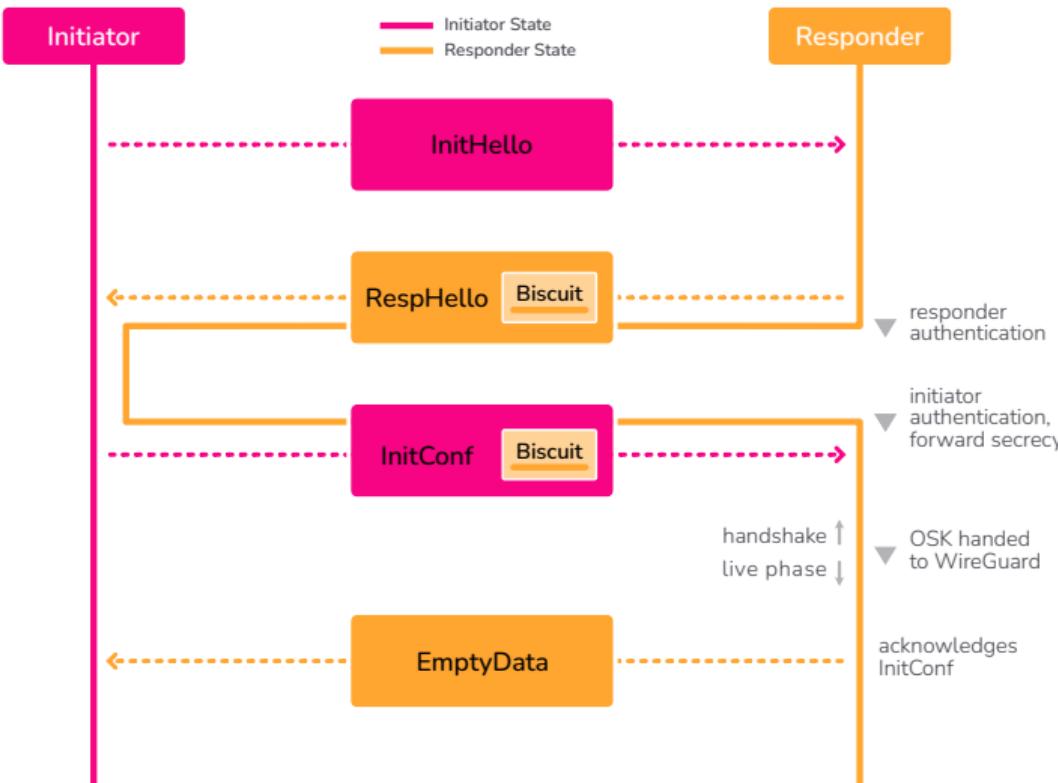


# Rosenpass Key Exchange Parts





# Rosenpass Protocol Features



- Authenticated key exchange
- Three KEM operations interleaved to achieve mutual authentication and forward secrecy
- No use of signatures
- First package (InitHello) is unauthenticated
- Stateless responder to avoid disruption attacks

# Hybridization

In the following slides you will learn ...

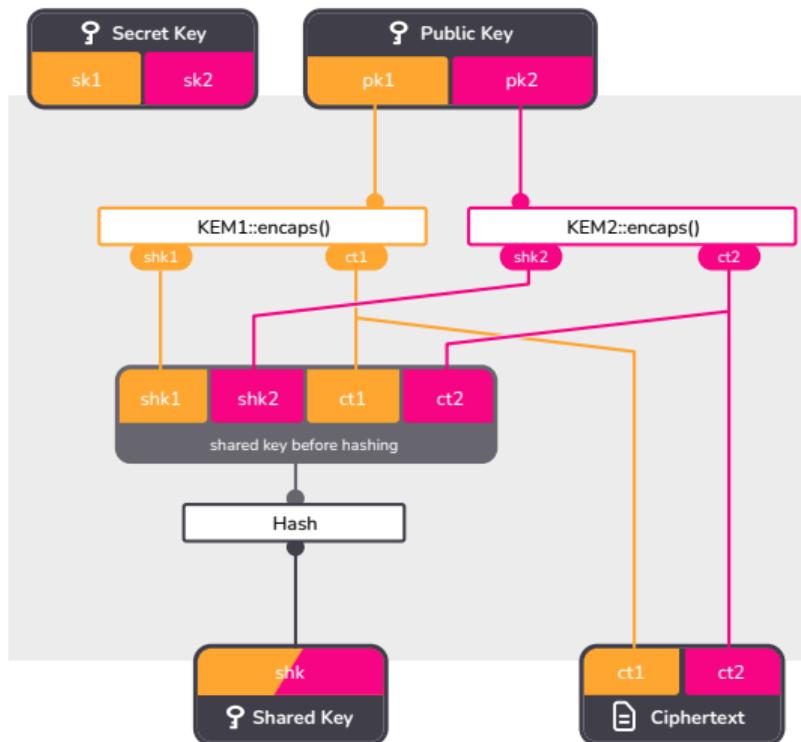
... that hybrid security can be achieved by building hybrid primitives and that it is not always wise to do so.





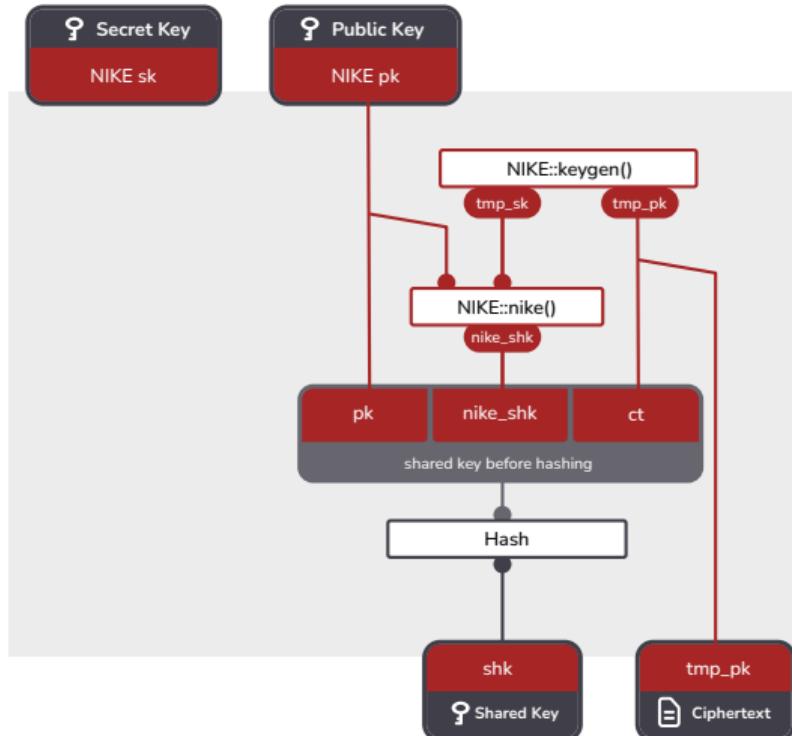
# Combining two KEMs with the GHP Combiner

- “Giacon-Heuer-Poettering” [GHP]
- Running both KEMs in parallel
- Secret keys, public keys, and ciphertexts are concatenated
- Shared keys are hashed together
- Ciphertexts included in hash for proof-related reasons





# Turning a NIKE into a KEM

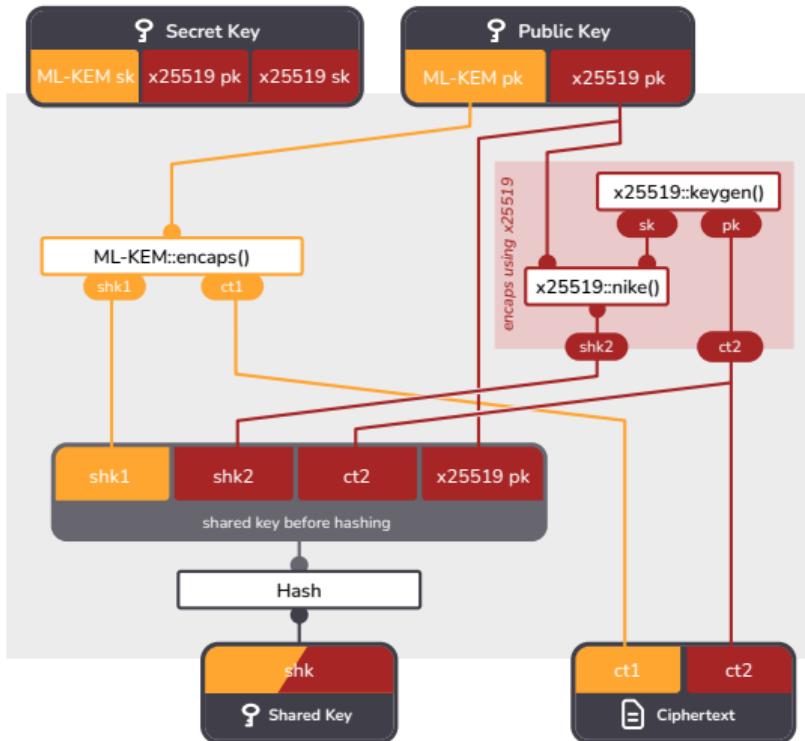


- From the HPKE RFC [HPKE]
- Remote keypair is static keypair
- Local keypair is temporary keypair
- Local keypair public key is treated as ciphertext
- For proof-related reasons, ciphertext and public key are included in hash
- Work by Blanchet, Hauck, Kiltz, Lipp, Riepel



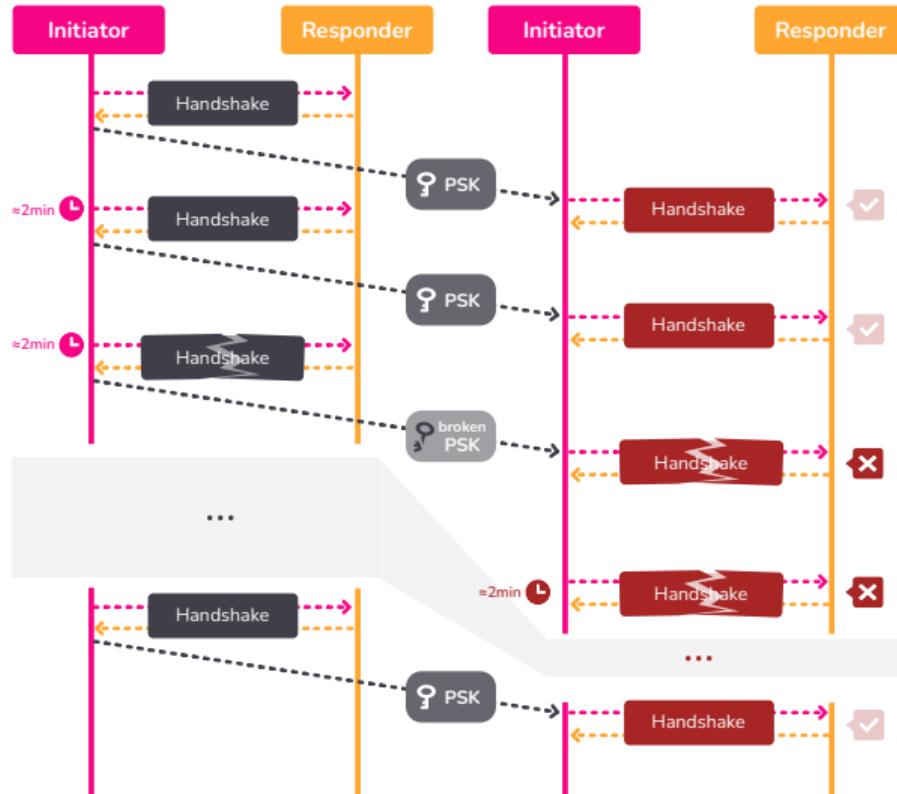
# X-Wing [XWING]

- Combines ML-KEM and x25519
- Techniques from DHKEM to turn x25519 into a KEM
- Techniques from GHP to combine the two
- Optimizations applied to make hashing more efficient
- Bespoke proof of security
- Work by Borbosa, Connolly, Duarte, Schwabe, Varner, Westerbaan





# Rosenpass & WireGuard Hybridization



- Rosenpass and WireGuard are hybridized on the protocol level
- Preserving efficiency of and trust in WireGuard
- Straightforward transition path; existing WireGuard implementation remains in use
- Key from Rosenpass used as PSK in WireGuard



# Full Protocol Reference in the Whitepaper

Initiator Code	Responder Code	Comments
1 <b>InitHello { sidi, epki, sctr, pidIC, auth }</b>	2      ↗	
Line   Variables ← Action	Variables ← Action	Line
RH1   ck ← lhash("chaining key init", spkr)	ck ← lhash("chaining key init", spkr)	IHR1
RH2   sidi ← random_session_id();		
RH3   eski, epki ← EKEM:keygen();		
RH4   mix(sidi, epki);	mix(sidi, epki)	IHR4
RH5   sctr ← encaps_and_mix<SKEM>(spkr);	decaps_and_mix<SKEM>(sskr, spkr, c11)	IHR5
RH6   pidIC ← encrypt_and_mix(pidC);	spki, psk ← lookup_peer(decrypt_and_mix(pidC))	IHR6
RH7   mix(spki, psk);	mix(spki, psk);	IHR7
RH8   auth ← encrypt_and_mix(empty());	decrypt_and_mix(auth)	IHR8
Comment		
Initialize the chaining key, and bind to the responder's public key.		
The session ID is used to associate packets with the handshake state.		
Generate fresh ephemeral keys, for forward secrecy.		
InitHello includes sidi and spki as part of the protocol transcript, and so we mix them into the chaining key to prevent tampering.		
Key encapsulation using the responder's public key. Mixes public key, shared secret, and ciphertext into the chaining key, and authenticates the responder.		
Tell the responder who the initiator is by transmitting the peer ID.		
Ensure the responder has the correct view on spki. Mix in the PSK as optional static symmetric key, with spki and spkr serving as nonces.		
Add a message authentication code to ensure both participants agree on the session state and protocol transcript at this point.		

4      ↙	<b>RespHello { sidr, sidi, ecti, scti, biscuit, auth }</b>	3      ↘
Line   Variables ← Action	Variables ← Action	Line
RH1   sidr ← random_session_id();	sidr ← random_session_id()	RH1
RH2   ck ← lookup_session(sidr);	mix(sidr, sidr);	RH2
RH3   mix(sidr, sidr);	ecti ← encaps_and_mix<EKEM>(epki);	RH3
RH4   decaps_and_mix<EKEM>(eski, epki, ecti);	scti ← encaps_and_mix<EKEM>(epki);	RH4
RH5   decaps_and_mix<SKEM>(sskr, spkr, scti);	scti ← encaps_and_mix<SKEM>(spki);	RH5
RH6   mix(biscuit)	biscuit ← store_biscuit();	RH6
RH7   decrypt_and_mix(auth)	auth ← encrypt_and_mix(empty());	RH7
Comment		
Responder generates a session ID.		
Initiator looks up their session state using the session ID they generated.		
Mix both session IDs as part of the protocol transcript.		
Key encapsulation using the ephemeral key, to provide forward secrecy.		
Key encapsulation using the initiator's static key, to authenticate the initiator, and non-forward-secret confidentiality.		
The responder transmits their state to the initiator in an encrypted container to avoid having to store state.		
Add a message authentication code for the same reason as above.		

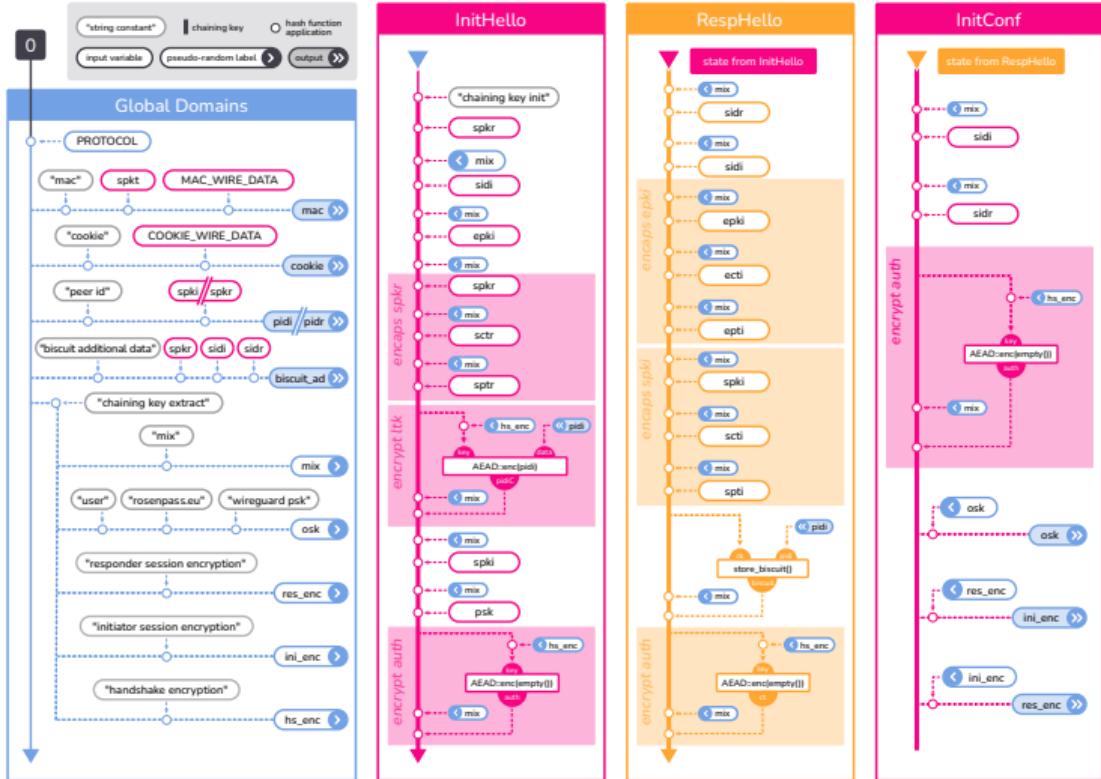
5      ↙	<b>InitConf { sidi, sidr, biscuit, auth }</b>	6      ↘
Line   Variables ← Action	Variables ← Action	Line
IC1	biscuit_no ← load_biscuit(biscuit);	ICR1
IC2	encrypt_and_mix(empty());	ICR2
IC3   mix(sidi, sidr);	mix(sidi, sidr);	ICR3
IC4   auth ← encrypt_and_mix(empty());	decrypt_and_mix(auth);	ICR4
IC5	assert(biscuit_no > biscuit_used);	ICR5
IC6	biscuit_used ← biscuit_no;	ICR6
IC7   enter_live();	enter_live();	ICR7
Comment		
Responder loads their biscuit. This restores the state from after RHR6.		
Responder recomputes RHR7, since this step was performed after biscuit encoding.		
Mix both session IDs as part of the protocol transcript.		
Message authentication code for the same reason as above, which in particular ensures that both participants agree on the final chaining key.		
Biscuit replay detection.		
Biscuit replay detection.		
Derive the transmission keys, and the output shared key for use as WireGuard's PSK.		

[rosenpass.eu/docs](https://rosenpass.eu/docs)

[rosenpass.eu/whitepaper.pdf](https://rosenpass.eu/whitepaper.pdf)



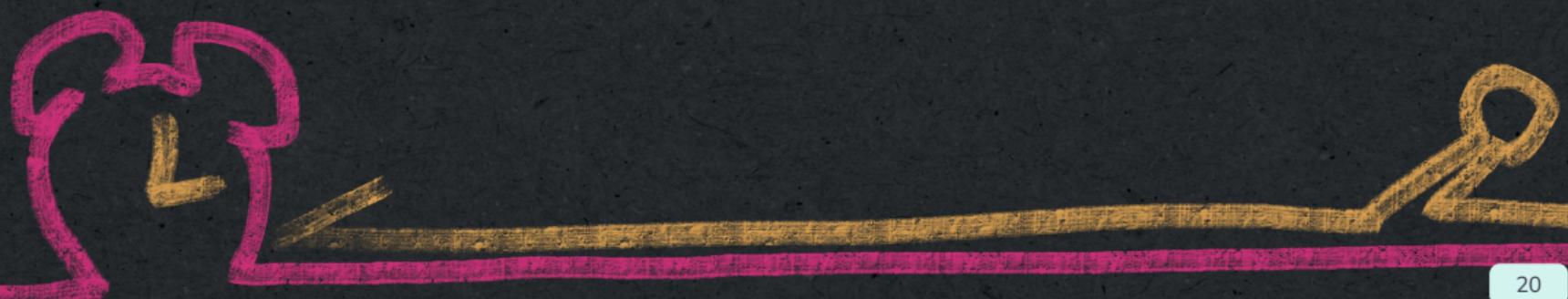
# Full Protocol Reference in the Whitepaper



[rosenpass.eu/docs](http://rosenpass.eu/docs)  
[rosenpass.eu/whitepaper.pdf](http://rosenpass.eu/whitepaper.pdf)

Trials ~ Attacks found

# ChronoTrigger



In the following slides you will learn ...

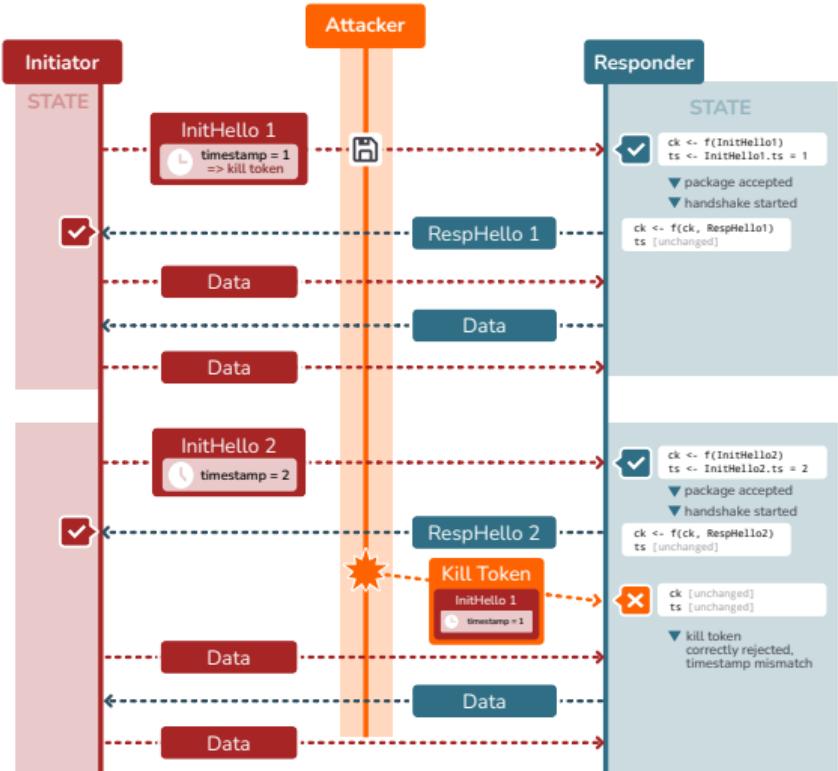
how to perform a protocol-level DoS attack against WireGuard, why wall clocks are not to be trusted and how to face replay attacks without fear.





# Retransmission Protection in WireGuard

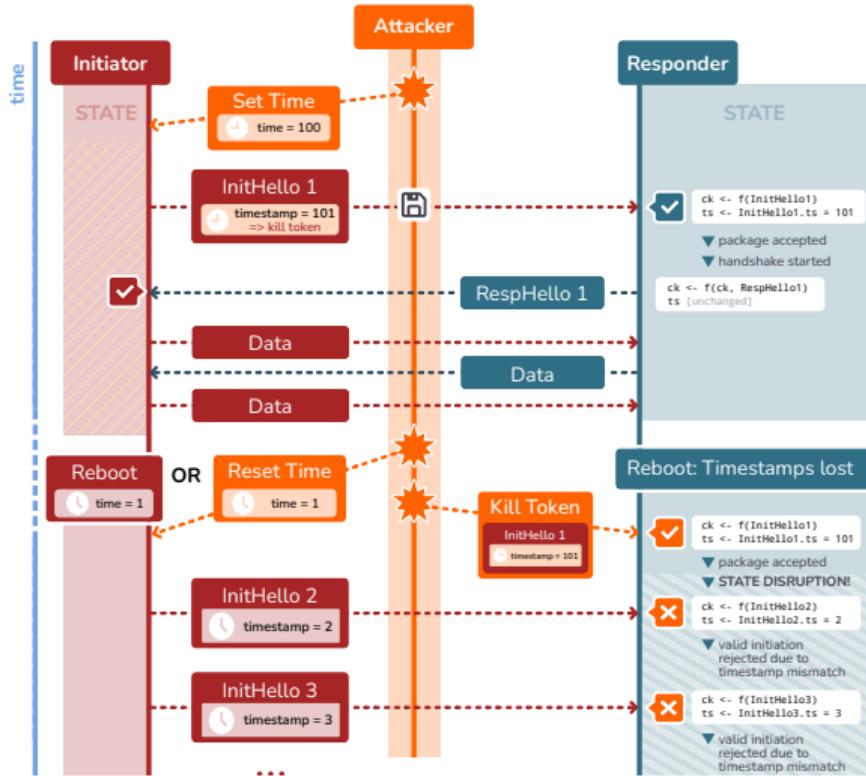
time



- Replay attacks thwarted by counter
  - Counter is based on real-time clock
  - Responder is semi-stateful (one retransmission at program start may be accepted, but this does not affect protocol security)
    - ⇒ WG requires *either* reliable real-time clock or stateful initiator
    - ⇒ Adversary can attempt replay, but this cannot interrupt a valid handshake by the initiator
- ! Assumption of reliable system time is 22



# ChronoTrigger Attack



## A. Preparation phase:

1. **Attacker** sets *initiator system time* to a future value
2. **Attacker** records *InitHello* as *KillToken* while both peers are performing a valid handshake

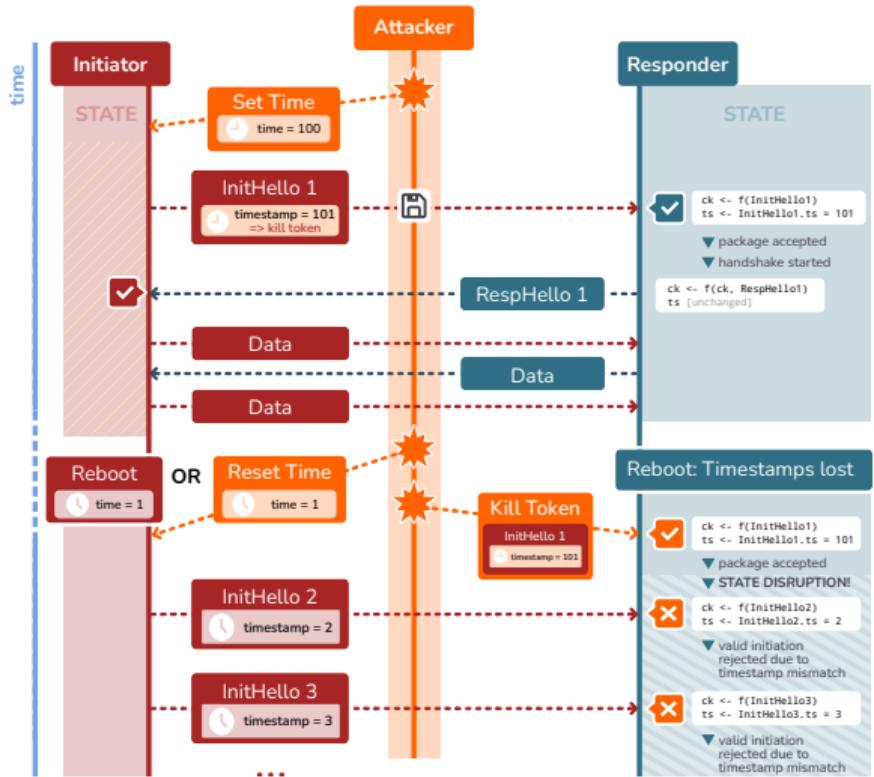
... both peers are being reset ...

## B. Delayed execution phase:

1. **Attacker** sends *KillToken* to responder, setting their timestamp to a future value
- ⇒ Initiation now fails again due to time mismatch



# ChronoTrigger Attack

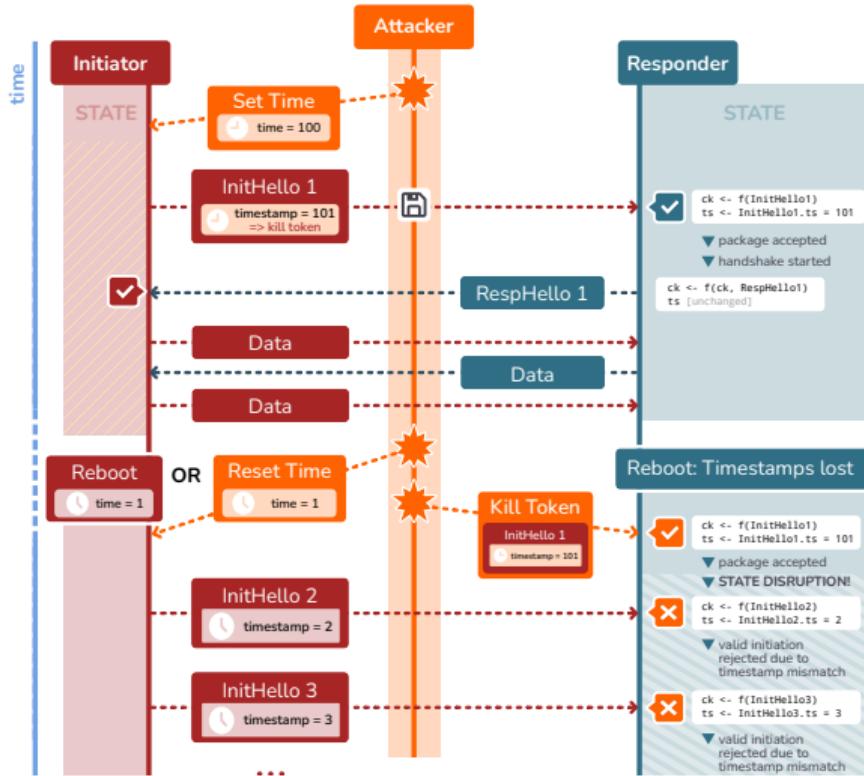


Gaining access to system time:

- Network Time Protocol is insecure, Mitigations are of limited use
- ⇒ Break NTP once; kill token lasts forever



# ChronoTrigger Attack



Attacker gains

- Extremely cheap protocol-level DoS

Preparation phase, attacker needs:

- Eavesdropping of initiator packets
- Access to system time

Delayed execution, attacker needs:

- No access beyond message transmission to responder



# What are State Disruption Attacks?

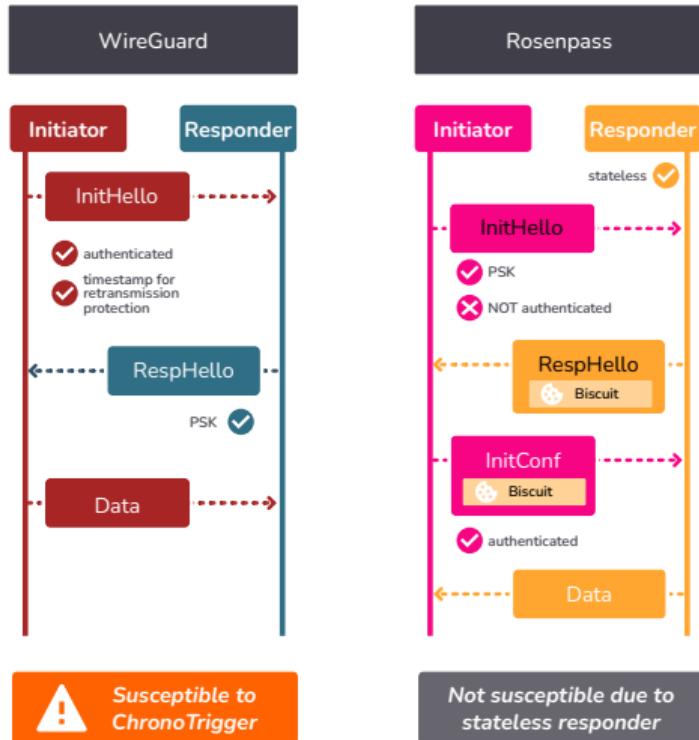


Protocol-level DoS





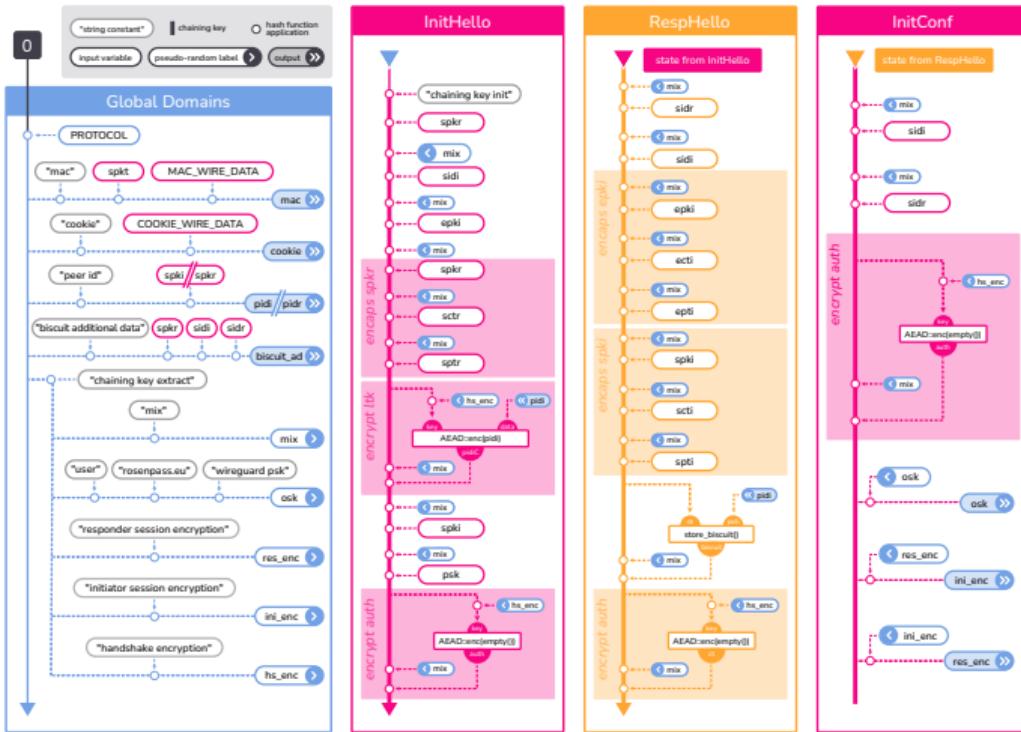
# ChronoTrigger: Changes in Rosenpass



- InitHello is unauthenticated because responder still needs to encapsulate secret with initiator key
  - Since InitHello is unauthenticated, retransmission protection is impossible
  - Responder state is moved into a cookie called *Biscuit*; this renders the responder stateless
  - Retransmission of InitHello is now easily possible, but does not lead to a state disruption attack
- ⇒ Stateless responder prevents ChronoTrigger attack



# Rosenpass Key Derivation Chain: Spot the Biscuit





# Rosenpass Protocol Messages: Spot the Biscuit

Envelope		bytes
type	1	
reserved	3	
<b>payload</b>	<b>n</b>	
mac	16	
cookie	16	
		<hr/>
envelope	$n + 36$	

COOKIE\_WIRE\_DATA  
MAC\_WIRE\_DATA

InitHello		type=0x81
sidi	4	
epki	800	
sctr	188	
pidiC	$32 + 16 = 48$	
auth	16	
		<hr/>
payload	1056	
+ envelope	1092	

RespHello		type=0x82
sidr	4	
sidi	4	
ecti	768	
scti	188	
<b>biscuit</b>	$76 + 24 + 16 = 116$	
auth	16	
		<hr/>
payload	1096	
+ envelope	1132	

InitConf		type=0x83
sidi	4	
sidr	4	
<b>biscuit</b>	$76 + 24 + 16 = 116$	
auth	16	
		<hr/>
payload	140	
+ envelope	176	

EmptyData		type=0x84
sid	4	
ctr	8	
auth	16	
		<hr/>
payload	28	
+ envelope	64	

Data		type=0x85
sid	4	
ctr	8	
<b>data</b>	<b>variable + 16</b>	
		<hr/>
payload	$variable + 28$	
+ envelope	$variable + 64$	

CookieReply		type=0x86
type(0x86)	1	
reserved	3	
sid	4	
nonce	24	
<b>cookie</b>	$16 + 16 = 32$	
		<hr/>
payload	64	

biscuit	
pidi	32
biscuit_no	12
ck	32
	<hr/>
biscuit	76
+ nonce	100
+ auth code	116

data nonce auth code



Tribulations ~ Tooling

# Oh These Proof Tools

Vive la Révolution! Against the

Bourgeoisie of Proof Assistants!



## Pen and Paper



Bellare and Rogaway: [BR06]

many “essentially unverifiable” proofs,  
“crisis of rigor”

Halevi: [Hal05]

some reasons are social,  
but “our proofs are truly complex”



# Symbolic Modeling of Rosenpass

```
~/p/rosenpass ➤ dev/karo/rwppc-slides ? ➤ nix build .#packages.x86_64-linux.p  
rosenpass-proverif> unpacking sources  
rosenpass-proverif> unpacking source archive /nix/store/cznyv4ibwlzbh257v6l  
rosenpass-proverif> source root is source  
rosenpass-proverif> patching sources  
rosenpass-proverif> configuring  
rosenpass-proverif> no configure script, doing nothing  
rosenpass-proverif> building  
rosenpass-proverif> no Makefile, doing nothing  
rosenpass-proverif> installing  
rosenpass-proverif> $ metaverif analysis/01_secrecy.entry.mpv -color -html  
-rosenpass-proverif  
rosenpass-proverif> $ metaverif analysis/02_availability.entry.mpv -color -  
ym6dv-rosenpass-proverif-proof  
rosenpass-proverif> $ wait -f 34  
rosenpass-proverif> $ cpp -P -I/build/source/analysis analysis/01_secrecy.e  
y.i.pv  
rosenpass-proverif> $ cpp -P -I/build/source/analysis analysis/02_availabil  
ity.entry.i.pv  
rosenpass-proverif> $ awk -f marzipan/marzipan.awk target/proverif/01_secre  
y  
rosenpass-proverif> $ awk -f marzipan/marzipan.awk target/proverif/02_avail  
ability  
rosenpass-proverif> 4s ✓ state coherence, initiator: Initiator accepting a  
lled the associated InitHello message  
rosenpass-proverif> 35s ✓ state coherence, responder: Responder accepting a  
lled the associated RespHello message  
rosenpass-proverif> 0s ✓ secrecy: Adv can not learn shared secret key  
rosenpass-proverif> 0s ✓ secrecy: There is no way for an attacker to learn  
rosenpass-proverif> 0s ✓ secrecy: The adversary can learn a trusted kem pk  
rosenpass-proverif> 0s ✓ secrecy: Attacker knowledge of a shared key implie  
rosenpass-proverif> 31s ✓ secrecy: Attacker knowledge of a kem sk implies t
```

- Symbolic modeling using ProVerif
- Proofs treated as part of the codebase
- Uses a model internally that is based on a fairly comprehensive Maximum Exposure Attacks (MEX) variant
- Covers non-interruptability (resistance to disruption attacks)
- Mechanized proof in the computational model is an open issue



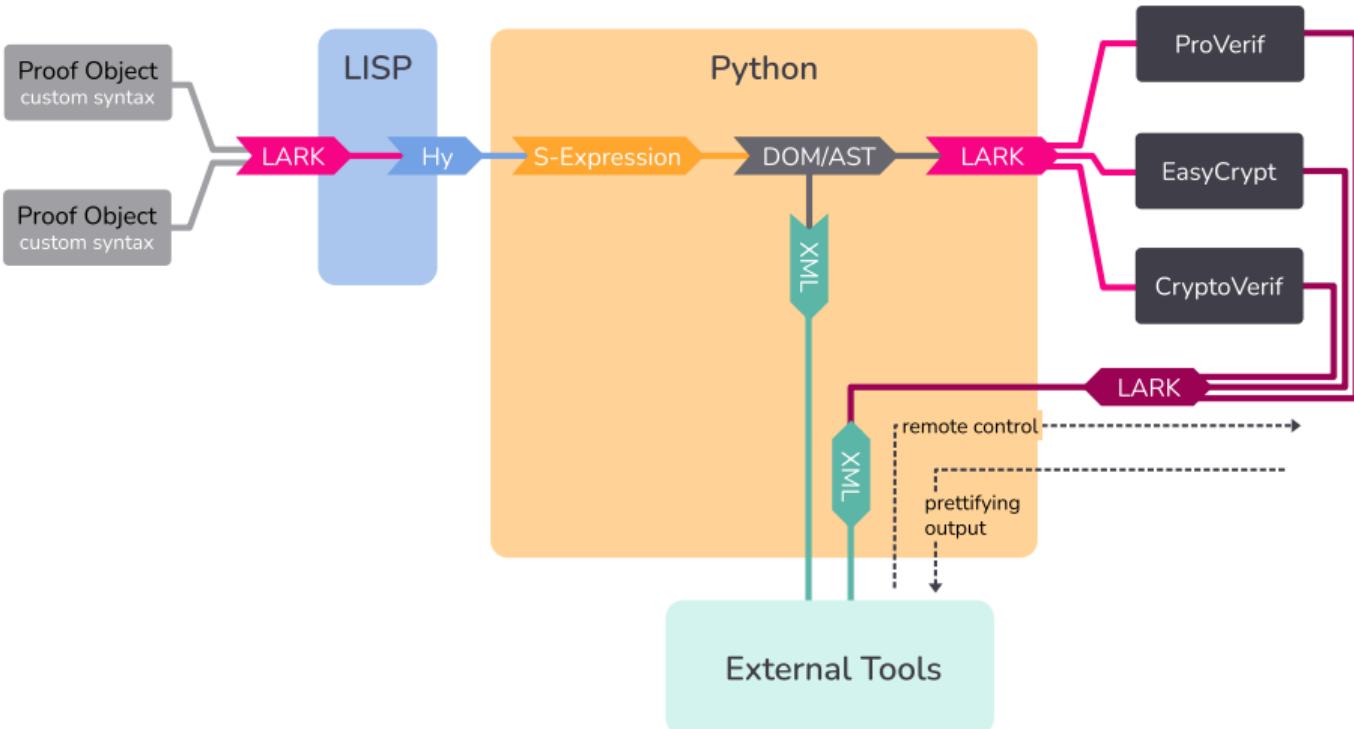
## The Day Language Came into My Life

Everything had a name, and each name gave birth to a new thought.

Helen Keller (1880-1968) in The Day Language Came into My Life



# Rosenpass going Rube-Goldberg



**Idea:** Build a framework around existing tools

**Keep** expressivity and preciseness

**Generate and parse** their languages

**Open them up to** ecosystems in Python, Lisp, XML

# Epilogue



## Epilogue

### Rosenpass

- Post-quantum secure AKE
- Same security as WireGuard
- Improved state disruption resistance
- Transfers key to WireGuard for hybrid security

### About Protocols

- It is possible to treat NIKEs as KEMs with DHKEM
- The GHP Combiner can be used to combine multiple KEMs
- X-Wing makes this easy
- Wall clocks are not to be trusted

### Talk To Us

- Adding syntax rewriting to the tool belt of mechanized verification in cryptography
- Using broker architectures to write more secure system applications
- Using microvms to write more secure applications
- More use-cases for

# Appendix — Here Be Dragons



## Bibliography

[PQWG]: <https://eprint.iacr.org/2020/379>

[GHP]: <https://eprint.iacr.org/2018/024>

[HPKE]: <https://eprint.iacr.org/2020/1499> &  
<https://datatracker.ietf.org/doc/rfc9180/>

[XWING]: <https://eprint.iacr.org/2024/039>



## Graphics attribution

- <https://unsplash.com/photos/brown-rabbit-Efj0HGPdPKs>
- <https://unsplash.com/photos/barista-in-apron-with-hands-in-the-pockets-standing-near-the-roaster-machine-Y5qjv6Dj4w4>
- [https://unsplash.com/photos/a-small-rabbit-is-sitting-in-the-grass-1\\_YMm4pVeSg](https://unsplash.com/photos/a-small-rabbit-is-sitting-in-the-grass-1_YMm4pVeSg)
- <https://unsplash.com/photos/yellow-blue-and-black-coated-wires-iOLHALaxpDA>
- <https://unsplash.com/photos/gray-rabbit-XG06d9Hd2YA>
- <https://unsplash.com/photos/big-ben-london-MdJq0zFUwrw>
- [https://unsplash.com/photos/white-rabbit-on-green-grass-u\\_kMWN-BWyU](https://unsplash.com/photos/white-rabbit-on-green-grass-u_kMWN-BWyU)
- <https://unsplash.com/photos/3-brown-bread-on-white-and-black-textile-WJDsVFwPjRk>
- <https://unsplash.com/photos/a-pretzel-on-a-bun-with-a-blue-ribbon-ymr0s7z6Ykk>
- <https://unsplash.com/photos/white-and-brown-rabbit-on-white-ceramic-bowl-rcfp7YEnJrA>

Random slides — The dragon just  
ate you!



## Rosenpass and WireGuard: Advanced Security

### Limited Stealth:

- Protocol should not respond without pre-auth.
- Proof of IP ownership (cookie mechanism) prevents full stealth
- Adv. needs to know responder public key

### CPU DoS mitigation:

- Attacker should not easily trigger public key operations
- Preventing CPU exhaustion using network amplification
- Proof of IP ownership

### Limited Identity Hiding:

- Adversary cannot recognize peers unless their public key is known
- This is incomplete!

Triumphs ~ Secrecy & Non-Interruptability

# Modeling of Rosenpass

Using ProVerif



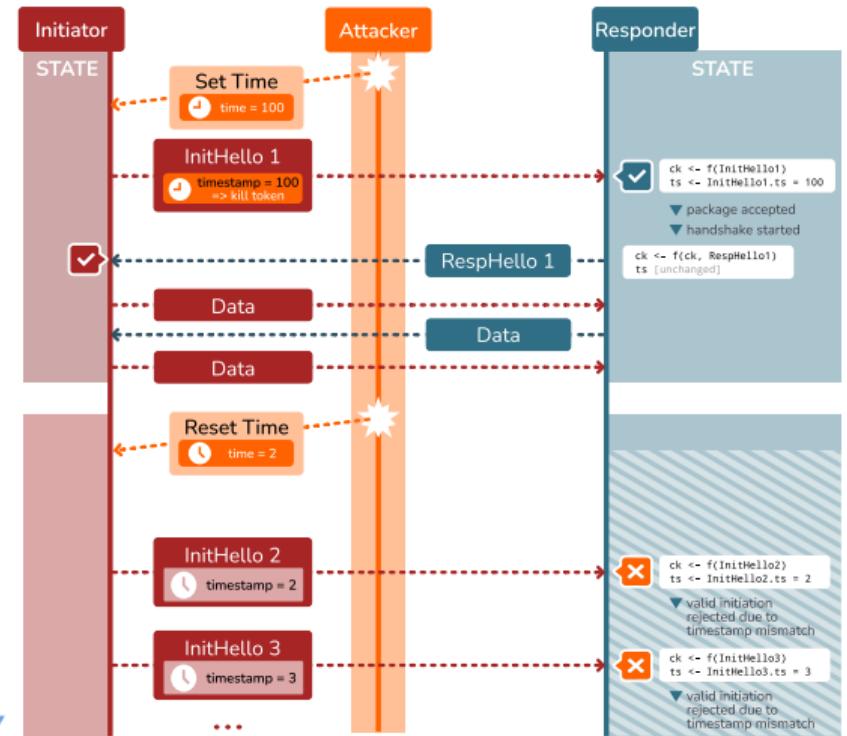
## Non-Interruptability: More Formally

For every pair of traces  $t_{\min}, t_{\max}$  where trace  $t_{\max}$  can be formed by insertion of messages/oracle calls into  $t_{\min}$ , the result of  $t_{\min}$  and  $t_{\max}$  should remain the same.

- Let  $\text{Result}$  be the set of possible protocol results
- Let  $\text{Trace}$  be the set of possible protocol traces
- Let  $\text{res}(t) : \text{Trace} \rightarrow \text{Result}$  determine the protocol result given  $t : \text{Trace}$
- Let  $t_1 \supseteq t_2 : \text{Trace} \rightarrow \text{Trace} \rightarrow \text{Prop}$  denote that  $t_2$  can be formed by insertion of elements into  $t_1$
- $\forall(t_{\min}, t_{\max}) : \text{Trace} \times \text{Trace}; t_{\min} \supseteq t_{\max} \rightarrow \text{res}(t_{\min}) = \text{res}(t_{\max})$



# ChronoTrigger Attack: Immediate Execution



## A. Preparation phase:

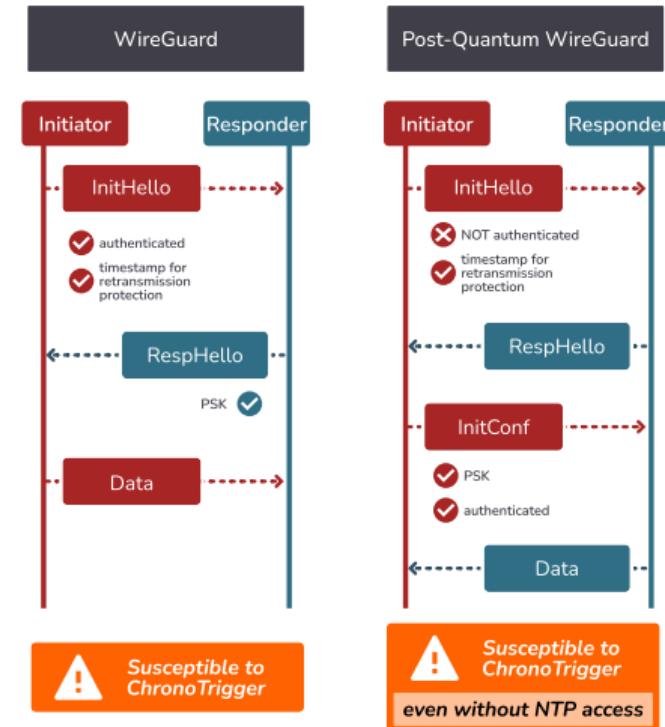
1. **Attacker** sets *initiator system time* to a future value
2. **Attacker** waits while both peers are performing a valid handshake

## B. Direct execution phase:

1. **Attacker** lets system time on initiator reset  
=> Initiation now fails due to counter mismatch



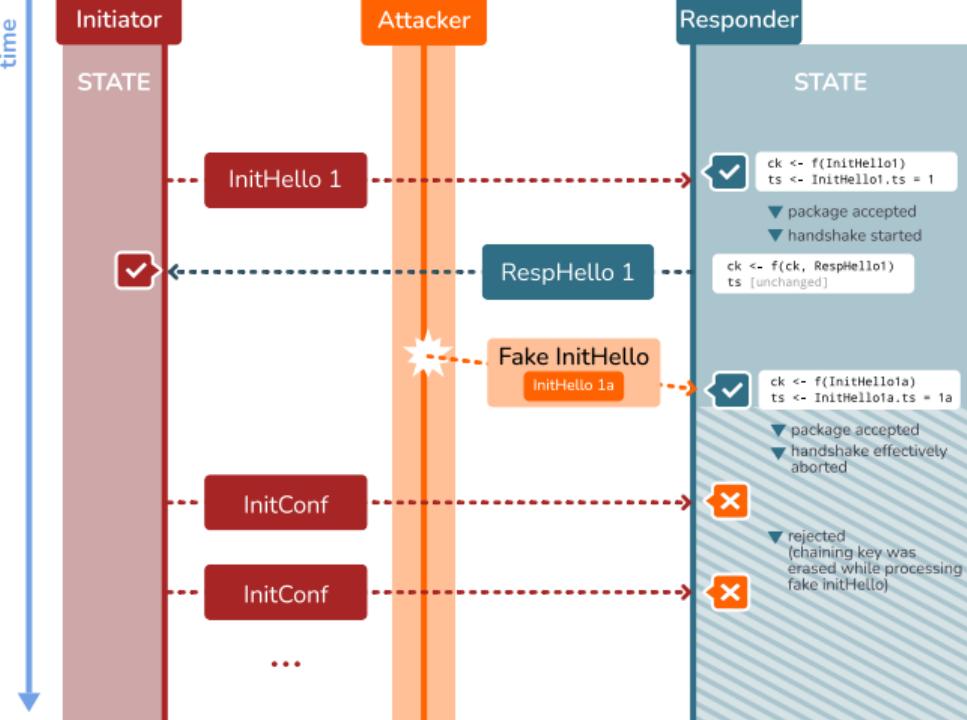
# ChronoTrigger: Changes in Post-Quantum WG



- *InitHello* is unauthenticated
- Retransmission counter is kept
- PQWG assumes a pre-shared key to authenticate *InitHello* instead (the authors recommend deriving the PSK from both public keys)
- PSK evaluated twice, during *InitHello* and *InitConf* processing



# ChronoTigger against Post-Quantum WireGuard



## No PSK/Public keys as PSK

- Attacker needs access to public keys
- The attack is trivial (attacker just forges *InitHello*)

## With PSK

- Replay attack with NTP access from classic WireGuard still applies



Trials ~ Attacks found

# CookieCutter



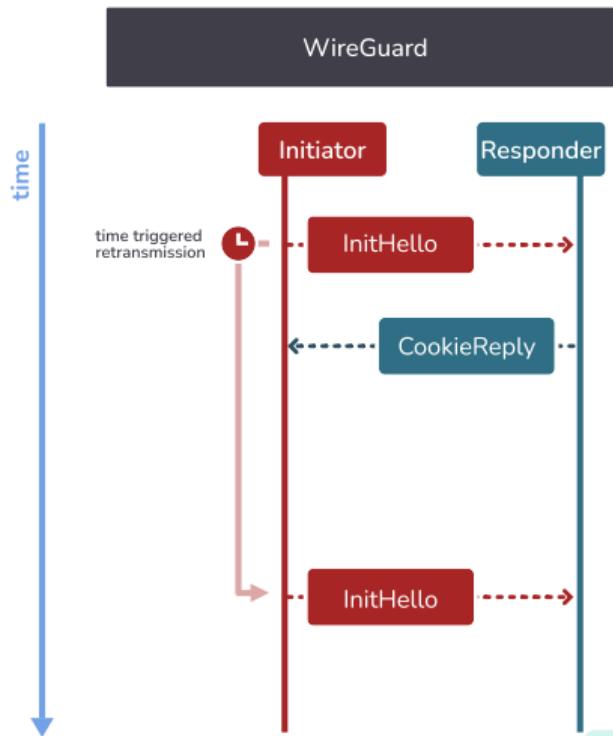


## CookieCutter Attack

I am under load. Prove that you are not using IP address impersonation before I process your handshake!

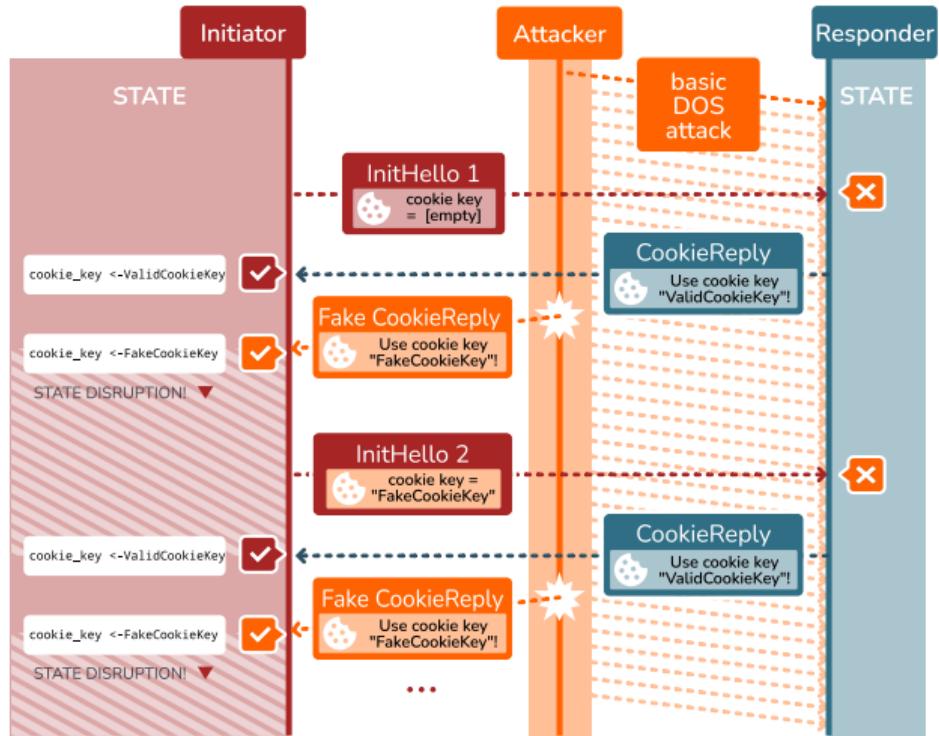
This message contains a *cookie* key. Use it to prove that you can receive messages sent to your address when retransmitting your *InitHello* packet.

A **WireGuard CookieReply**, ca. 2014





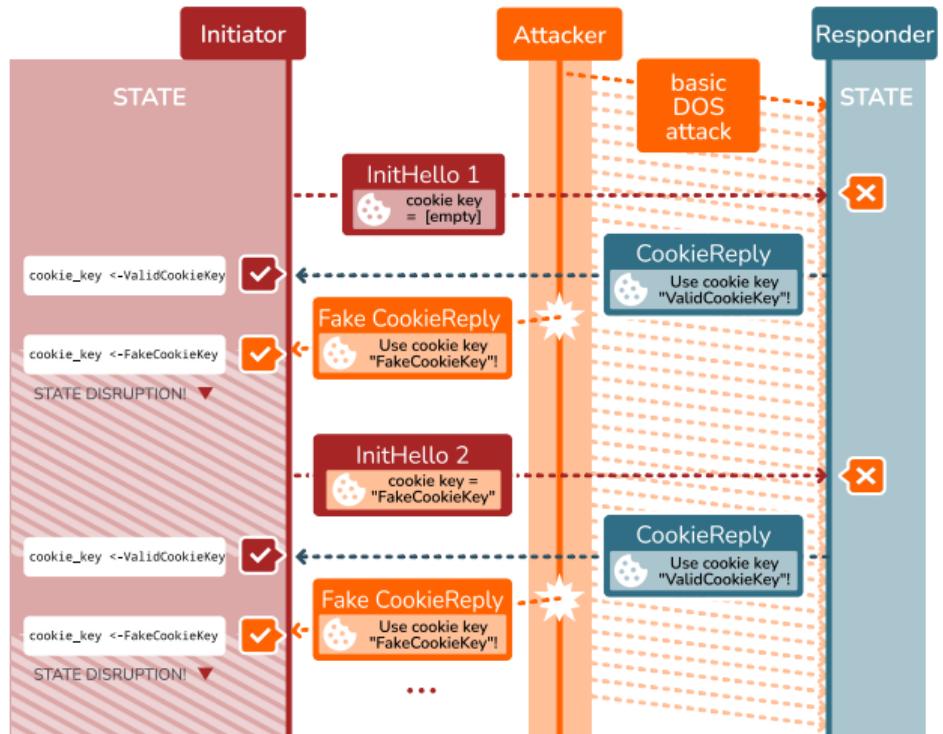
# CookieCutter Attack



1. **Attacker** begins continuous DoS attack against responder
2. **Initiator** begins handshake, sends *InitHello*
3. **Responder** replies with **CookieReply**  
**CookieReply:** I am under load.  
 Prove you are not using an IP spoofing attack with this cookie key.
4. **Initiator** Initiator stores cookie key and waits for their retransmission timer
5. **Attacker** forges a cookie reply with a fake cookie key
6. **Initiator** Initiator overwrites the valid



# CookieCutter Attack



Attacker gains:

- Cheap protocol-level DoS

Attacker needs:

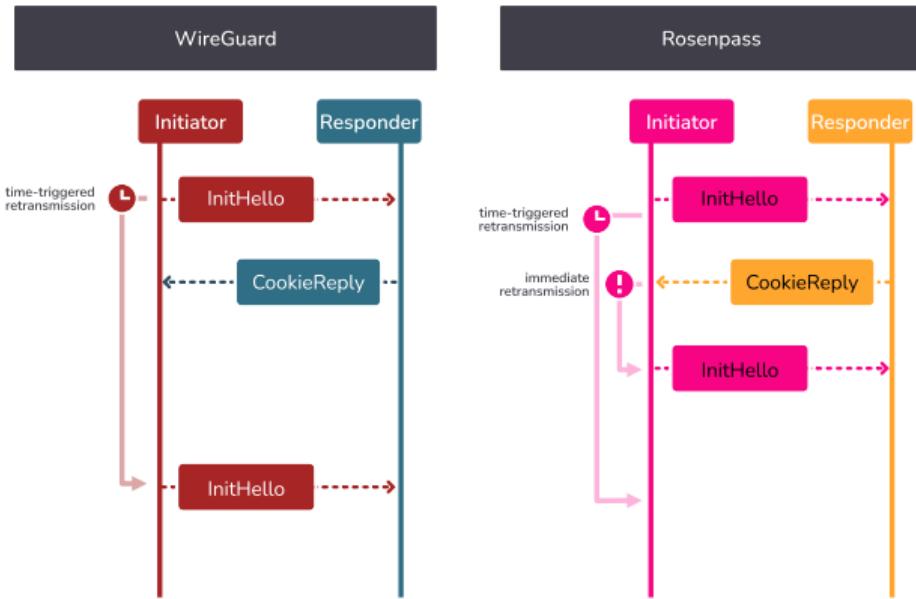
- Knowledge of public keys
- Good timing

Role switching:

- WireGuard sometimes uses role switching
- To account for that, the attack can be performed against both peers



# CookieCutter: Post-Quantum WG & Rosenpass



Susceptible to CookieCutter

Not susceptible due to immediate retransmission upon *CookieReply*

*InitHello* and *CookieReply* must be of same size to avoid amplification DOS attacks

## Post-Quantum WireGuard

- No change.

## Rosenpass

- Immediate retransmission of *InitHello* upon receiving *CookieReply*
  - CookieReply* and *InitHello* must be of same size to prevent DoS amplification attacks
- ⇒ Rosenpass is protected from CookieCutter attacks

Trials ~ Advanced Security Properties

# Knock Patterns





## Rosenpass and WireGuard: Advanced Security

### CPU DoS mitigation:

- No change on the protocol level.
- Slightly worsened in practice because PQ operations are more expensive than elliptic curves

### Limited Stealth:

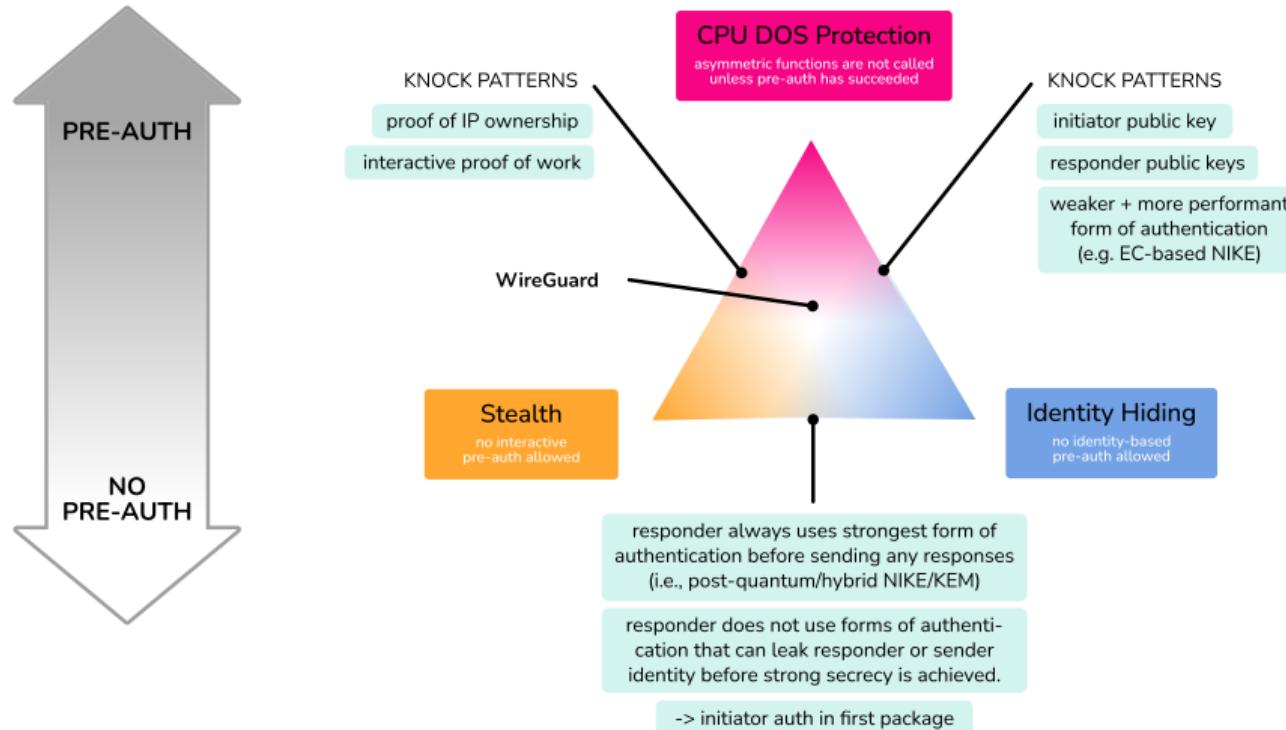
- No change in Rosenpass, but we should have **full stealth!**
  - ⇒ Remove cookie mechanism?
- This would affect the CPU DoS mitigation too much.

### Limited Identity Hiding:

- No change in Rosenpass, but we should have **full identity hiding!**
  - ⇒ Do not use pre-authentication with public key?
- This would affect the CPU DoS mitigation, possibly too much.

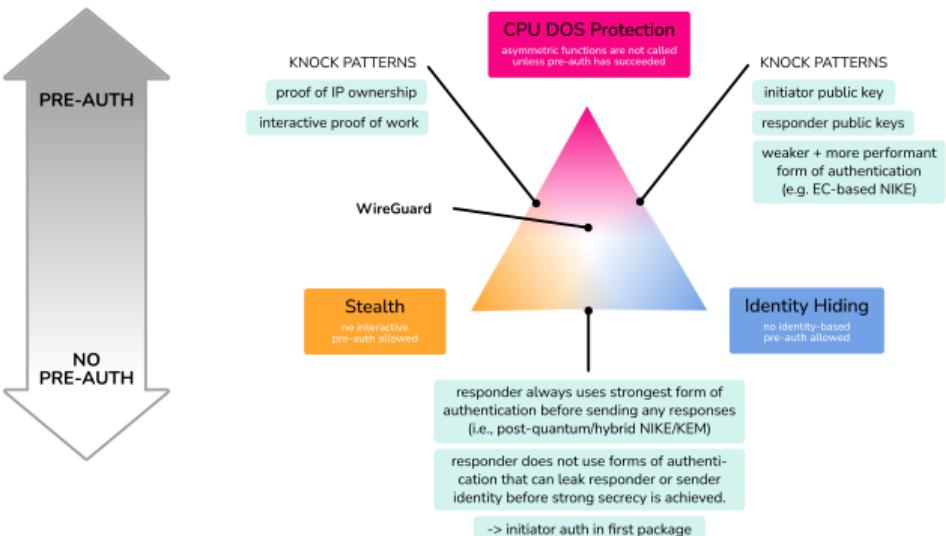


## Choose Two: Stealth, Identity Hiding, CPU DoS Mit.





# WireGuard and Rosenpass Trade-Offs



## CPU DoS Mitigation:

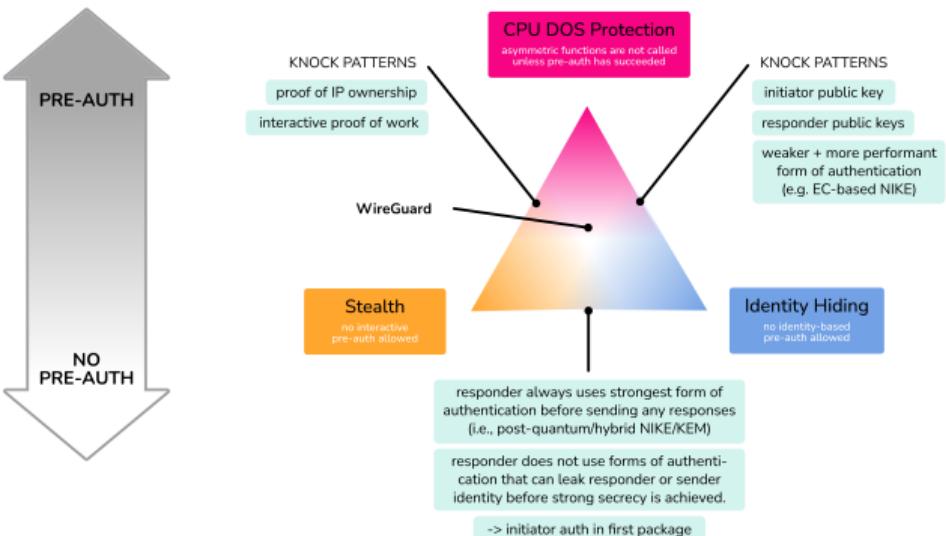
- There is no clear optimum here.
- CPU DoS mitigation is never calling asymmetric crypto unless we know it succeeds (circular reasoning)

## Stealth:

## Identity hiding:



# WireGuard and Rosenpass Trade-Offs



## CPU DoS Mitigation:

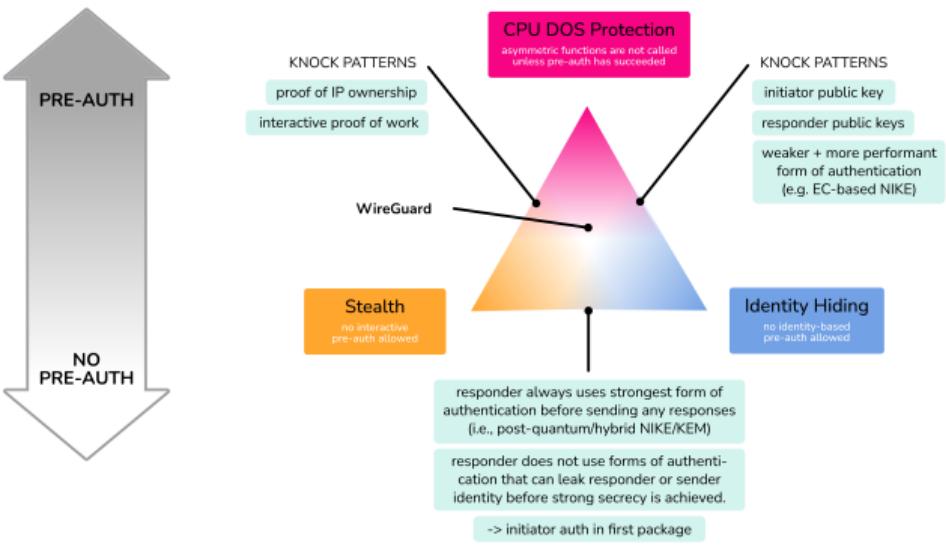
### Stealth:

- Broken on DoS attacks assuming recipient is known
- ⇒ This seems acceptable

### Identity hiding:



# WireGuard and Rosenpass Trade-Offs



CPU DoS Mitigation:

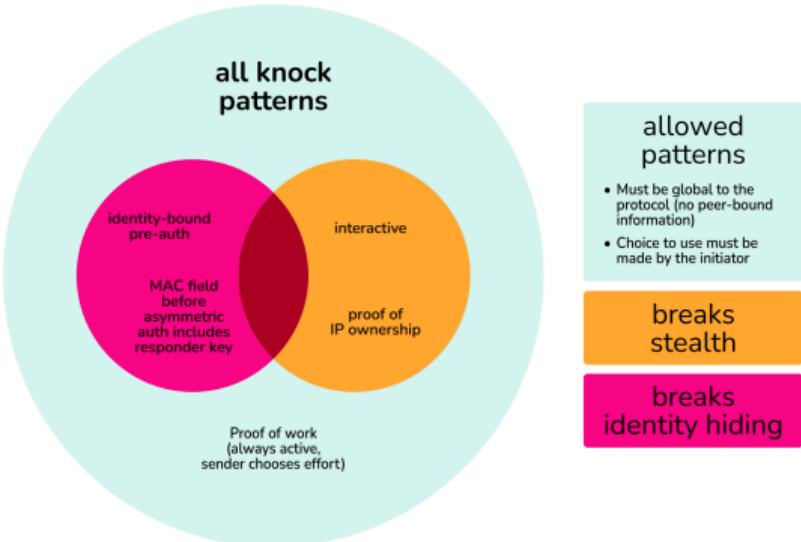
Stealth:

Identity hiding:

- Broken on knowledge of public keys
- ⇒ This seems unacceptable!
- ⇒ Investigate proper identity hiding without overly impacting stealth and CPU DoS mitig.



# Knock Patterns



- We choose to think of WireGuard's and Rosenpass' pre-auth as "Knock Patterns"
  - These knock patterns have severe trade-offs.
  - Interactive knock pattern (cookie mechanism) breaks stealth
  - Identity-based knock patterns (e.g., knowledge of public key) breaks identity hiding
- ⇒ Avoid identity-bound knock patterns
- ⇒ Minimize interactive knock patterns
- ⇒ Explore other (allowed) knock patterns



## Tools to the Table!

Bellare and Rogaway [BR06], Halevi [Hal05]:

Call for “automated tools, that can help write and verify game-based proofs”



## Tools to the Table!

Bellare and Rogaway [BR06], Halevi [Hal05]:

Call for “automated tools, that can help write and verify game-based proofs”

Do the tools *actually help?* And if yes, whom?

ProVerif, Tamarin, CryptoVerif, EasyCrypt:

We like these tools, they are good!



## Tools to the Table!

Bellare and Rogaway [BR06], Halevi [Hal05]:

Call for “automated tools, that can help write and verify game-based proofs”

Do the tools *actually help?* And if yes, whom?

ProVerif, Tamarin, CryptoVerif, EasyCrypt:

We like these tools, they are good!

They mostly help the *formal verification experts* to:

- do analyses themselves, write papers
- develop proof methodologies, foundation work for formal methods

# Epilogue

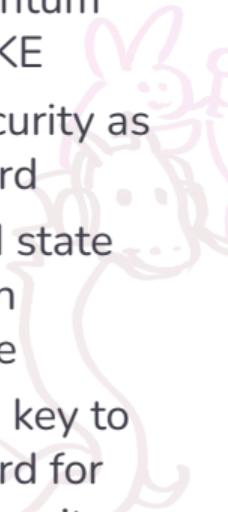




# Conclusion

## Rosenpass

- Post-quantum secure AKE
- Same security as WireGuard
- Improved state disruption resistance
- Transfers key to WireGuard for hybrid security



## Protocol Findings

- **CookieCutter**: DoS exploiting WireGuard cookie mechanism
- **ChronoTrigger**: DoS exploiting insecure system time to attack WireGuard
- There is a **trade-off** between identity hiding, stealth, and CPU-exhaustion DoS protection

## Talk To Us

- About why we should use Tamarin (or SAPIC+?) over ProVerif
- State disruption attacks
- Stealth and Identity hiding
- Adding syntax rewriting to the tool belt of mechanized verification in cryptography



## Rosenpass going Rube-Goldberg: The Details

- Embed cryptographic proof syntax in Lisp S-Expressions
- Translate Lisp code to Python using the Hy language (Lisp that compiles to Python)
- Translate S-Expression code to AST or DOM
- Translate AST or DOM to ProVerif/Tamarin/CryptoVerif/EasyCrypt code using the LARK code parser/generator
- Remote control ProVerif/Tamarin/CryptoVerif/EasyCrypt by
  - Parsing their command line output using LARK
  - (Possibly using the language server interface for more interactive features)
- Provide custom syntax using
  - Lisp Macros
  - Extending LARK-based syntax parsers (to add custom syntactic elements)