



PQC Wireguard as a new VPN

Philip Kastura-Sahl
Universität Heidelberg

Wireguard



- Handshake every two minutes
- Handshake based on Diffie-Hellman
- Uses pre-Quantum ciphers

Rosenpass



- Post-quantum Encryption/Decryption in the wild!
- Spiritual Successor to PQ Wireguard
- Why? Because store now, decrypt later.



Huh?

Encryption using AES-CBC with a 256-bit key with "CS1" ciphertext stealing.

```
int encrypt(const unsigned char *key, const unsigned char *iv,
            const unsigned char *msg, size_t msg_len, unsigned char *out)
{
    /*
     * This assumes that key size is 32 bytes and the iv is 16 bytes.
     * For ciphertext stealing mode the length of the ciphertext "out" will be
     * the same size as the plaintext size "msg_len".
     * The "msg_len" can be any size >= 16.
     */
    int ret = 0, encrypt = 1, outlen, len;
    EVP_CIPHER_CTX *ctx = NULL;
    EVP_CIPHER *cipher = NULL;
    OSSL_PARAM params[2];

    ctx = EVP_CIPHER_CTX_new();
    cipher = EVP_CIPHER_fetch(NULL, "AES-256-CBC-CTS", NULL);
    if (ctx == NULL || cipher == NULL)
        goto err;

    /*
     * The default is "CS1" so this is not really needed,
     * but would be needed to set either "CS2" or "CS3".
     */
    params[0] = OSSL_PARAM_construct_utf8_string(OSSL_CIPHER_PARAM_CTS_MODE,
                                                  "CS1", 0);
    params[1] = OSSL_PARAM_construct_end();

    if (!EVP_CipherInit_ex2(ctx, cipher, key, iv, encrypt, params))
        goto err;

    /* NOTE: CTS mode does not support multiple calls to EVP_Cipherupdate() */
    if (!EVP_Cipherupdate(ctx, out, &outlen, msg, msg_len))
        goto err;
    if (!EVP_CipherFinal_ex(ctx, out + outlen, &len))
        goto err;
    ret = 1;

err:
    EVP_CIPHER_free(cipher);
    EVP_CIPHER_CTX_free(ctx);
    return ret;
}
```

Get Siked!

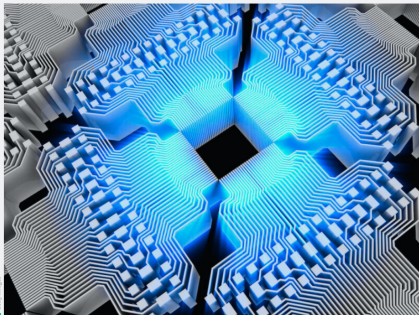
ars TECHNICA[ART & IT](#) [TECH](#) [SCIENCE](#) [POLICY](#) [CARS](#) [GAMING & CULTURE](#) [STORE](#) [FORUMS](#) [SUBSCRIBE](#) [SIGN IN](#)

COULDA BEEN A CONTENDER —

Post-quantum encryption contender is taken out by single-core PC and 1 hour

Leave it to mathematicians to muck up what looked like an impressive new algorithm.

DAN GOODIN · 8/2/2022, 2:31 PM

[Enlarge](#)

In the US government's ongoing campaign to protect data in the age of quantum computers, a new and powerful attack that used a single traditional computer to completely break a fourth-round candidate highlights the risks involved in standardizing the next generation of encryption algorithms.



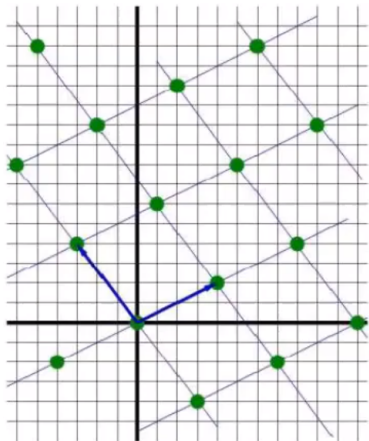
Which Ciphers does Rosenpass use?

- **Classic McEliece** for Authentication and confidentiality (linear code based)
- **Kyber** for Forward Secrecy (lattice based)
- notably both are NIST¹ PQC Standardization Round 3 Finalists

¹ „National Institute of Standards and Technology“ – NIST

Kyber

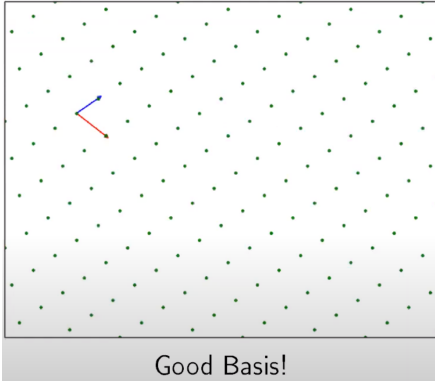
Lattices & Basis



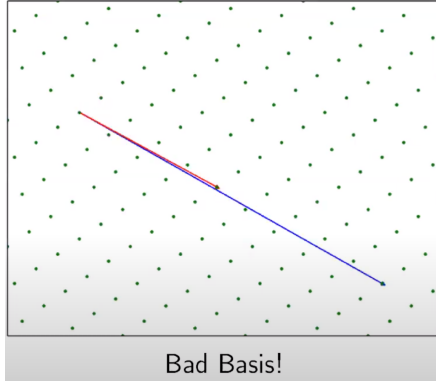
$$L = z_1 b_1 + z_2 b_2 = \begin{bmatrix} 4 & -3 \\ 2 & 4 \end{bmatrix} \cdot \begin{bmatrix} z_1 \\ z_2 \end{bmatrix}$$



Kyber Lattices – CVP²



Good Basis!

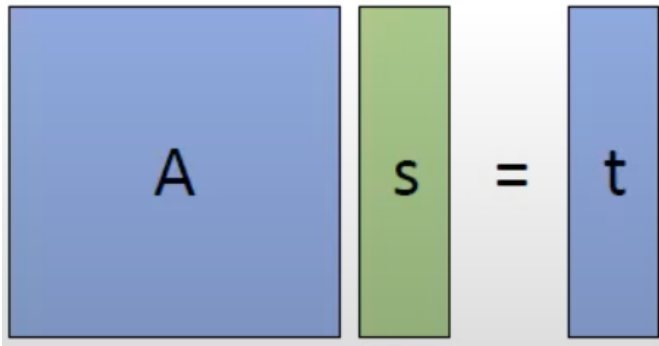


Bad Basis!

² „Closest vector problem“ – CVP

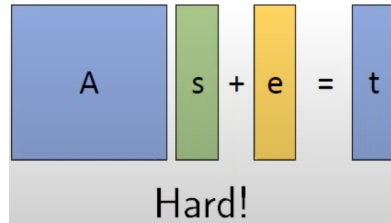
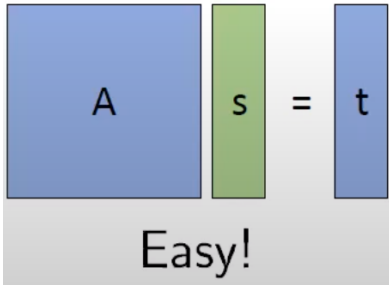


Kyber LWE





Kyber LWE³



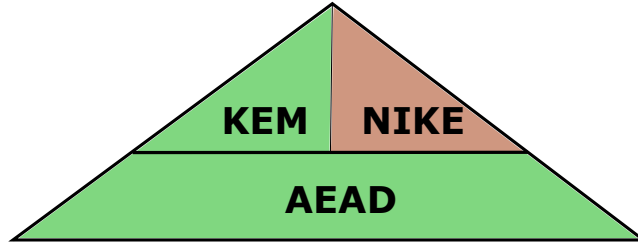
³ „Learning with Errors“ – LWE



Ciphers available PQC⁴

Asymmetrisch

Symmetrisch



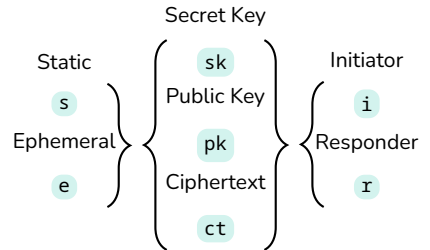
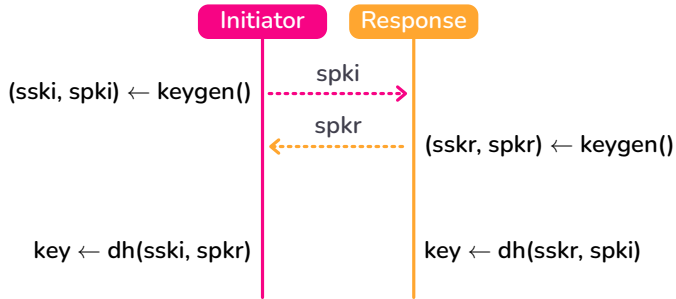
■ Nicht verfügbar

■ Verfügbar

⁴ „Post-quantum cryptography“ – PQC



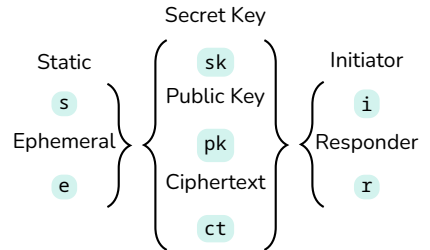
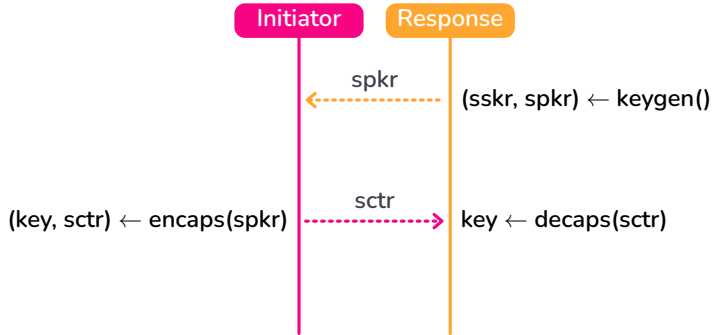
NIKE⁵



⁵ „Non-Interactive Key Exchange“ – NIKE



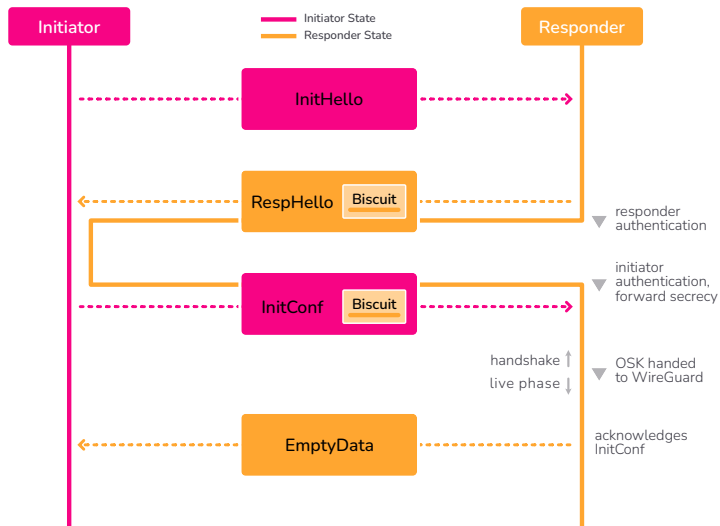
KEM⁶



⁶ „Key-Encapsulation Method“ – KEM

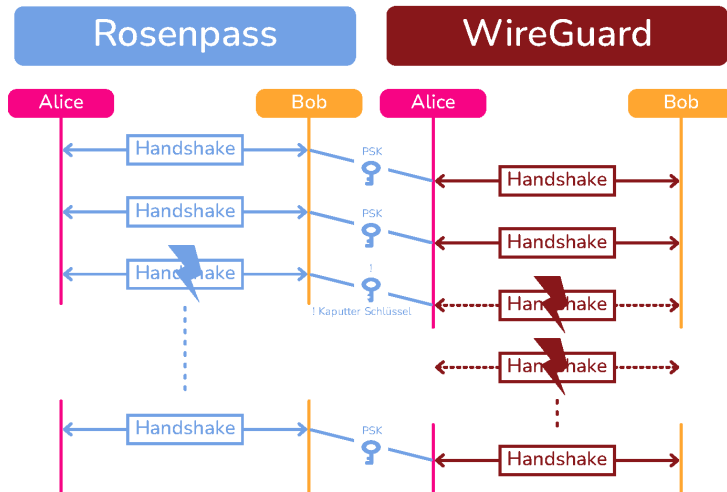


Rosenpass Key Exchange





Wireguard Integration







Question 1:

- Do you think Rosenpass has a future if PQ Ciphers establish themselves?
-



Question 1:

- Do you think Rosenpass has a future if PQ Ciphers establish themselves?
- Hint: 'Technical Dept'



Question 2:

- The Rosenpass developers may allow you to choose your own ciphers in the future. Why would they **not** enable this?
-



Question 2:

- The Rosenpass developers may allow you to choose your own ciphers in the future. Why would they **not** enable this?
- Hint: They definitely won't allow for **dynamic negotiation** of ciphers between initiator and responder.



Question 3:

- Despite this, why would Administrators 'choose' to pick different ciphers?
-



Question 3:

- Despite this, why would Administrators 'choose' to pick different ciphers?
- Hint: National Institute of Standards and Technology (NIST)