Post-Quantum Code-Based Cryptosytems

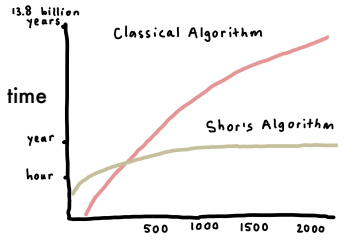
in search for new public-key cryptography standards

Lola Dekhuijzen

1. background

Shor's Algorithm

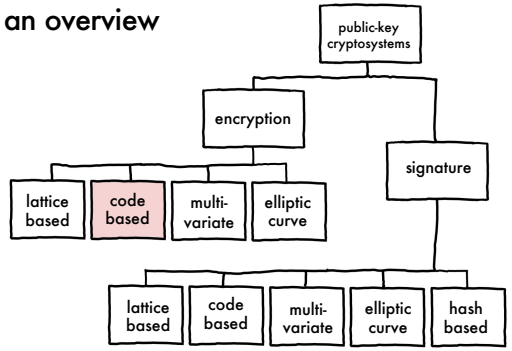
how quantum computers will break RSA



digits of to be factorized number

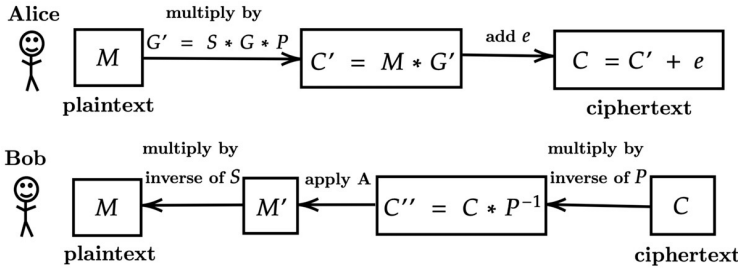
Post-Quantum Cryptography

an overview



McEliece (1978)

the first code-based cryptosystem



Alice wants to send a message to Bob using the McEliece cryptosystem. She chooses some linear code with efficient decoding algorithm A and generator matrix G.

2. method

Research Method

compare all schemes and decide on which scheme has the most potential.

for each scheme:

- study the specification
- evaluate security and cost
- assess performance by re-implementing source code

3. results

	public key	private key	cipher text
Classic McEliece	1357824	14120	240
BIKE	5122	580	5154
LEDAcrypt	4424	2232	4464
HQC	7245	40	14469
RQC	4090	40	8164

bandwidth in bytes for 256-bit security

the importance of a low Decoding Failure Rate (DFR)

- gives the adversary information about the secret key.
- the GJS key recovery attack exploits decoding failures.
- requirement of Fujisaki-Okamoto transform: go from CPA- to CCA-security.

Classic McEliece	BIKE	LEDAcrypt	HQC	RQC
zero	$\sim 2^{-\lambda}$	$2^{-\lambda}$	$2^{-\lambda}$	zero

λ: security level

	keygen	encaps	decaps
Classic McEliece	541 489 441	178 093	326 531
BIKE	1 780 000	465 000	6 610 000
LEDAcrypt	34 592 000	1 919 300	15 640 700
HQC	423 000	738 000	1 286 000
RQC	2 860 000	5 270 000	36 390 000

performance in cycles

Classic McEliece

using binary Goppa codes

+ fast encapsulation and decapsulation
+ small cipher texts (useful for some applications)
– large public keys

BIKE

using QC-MCDC codes

+ reasonable key sizes
– estimated DFR

HQC

using Hamming codes

+ security not directly related to how well the structure of an error-correcting code can be hidden
+ faster than BIKE
– worse bandwidth than BIKE

RQC

using Rank codes

+ security not directly related to how well the structure of an error-correcting code can be hidden
+ null DFR
– decryption speed

4. conclusion

- Classic McEliece is secure and ready for specific use cases.
- Quasi-cyclic codes lead to better public key sizes.
- Rank-metric has smaller key sizes than Hamming-metric but partially because its attacks have not been researched enough.

TU Delft