Quantum Safe Cryptography on IBM zSystems

—

Nico Einsidler
Technical Specialist IBM zSystem
IBM Quantum Ambassador

Physics → Quantum Safe Cryptography ← Computer Science

Agenda

motivation
cryptography
quantum-safe algorithms on zSystems

Quantum 101 & Update

opportunity

thread

Cryptography

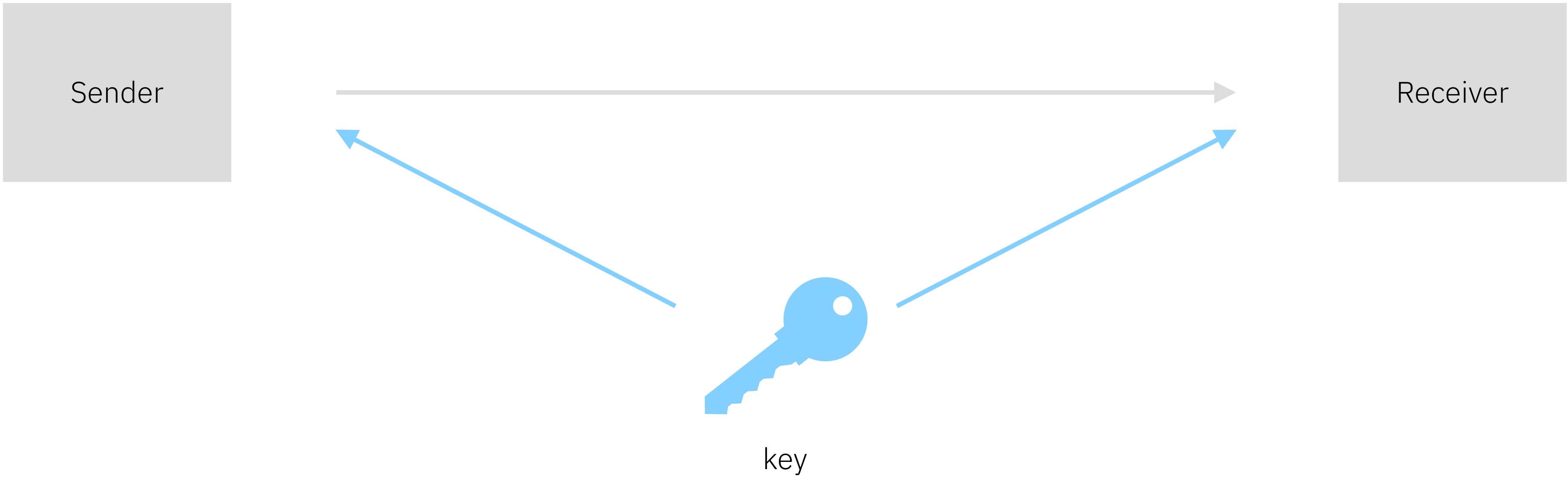
– confidentiality

– integrity

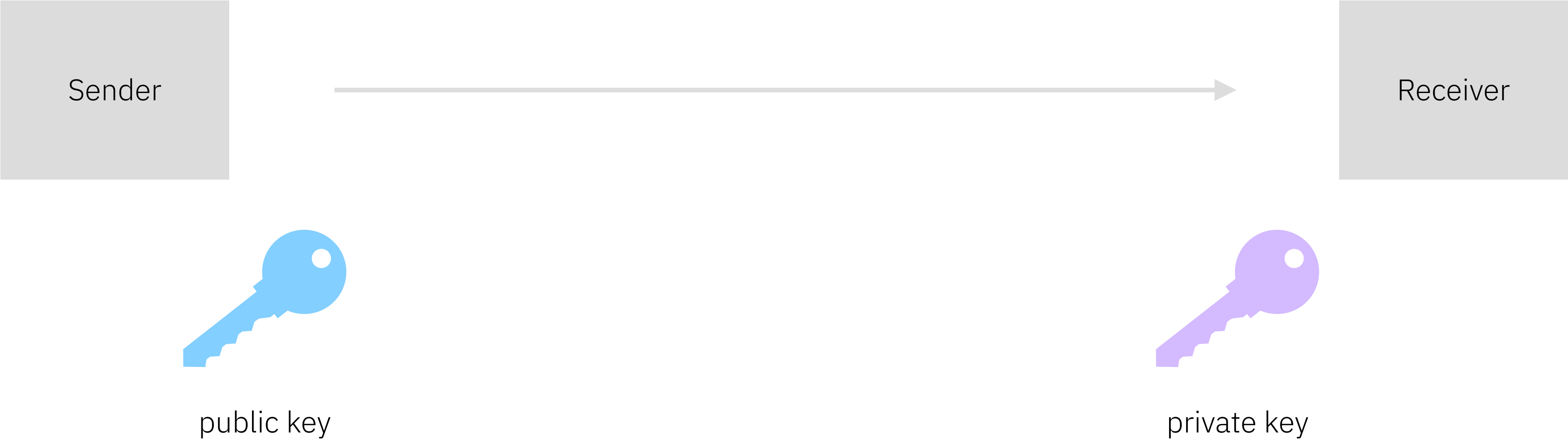
– authenticity

– non repudiation

Symmetric Cryptography



Asymmetric Cryptography



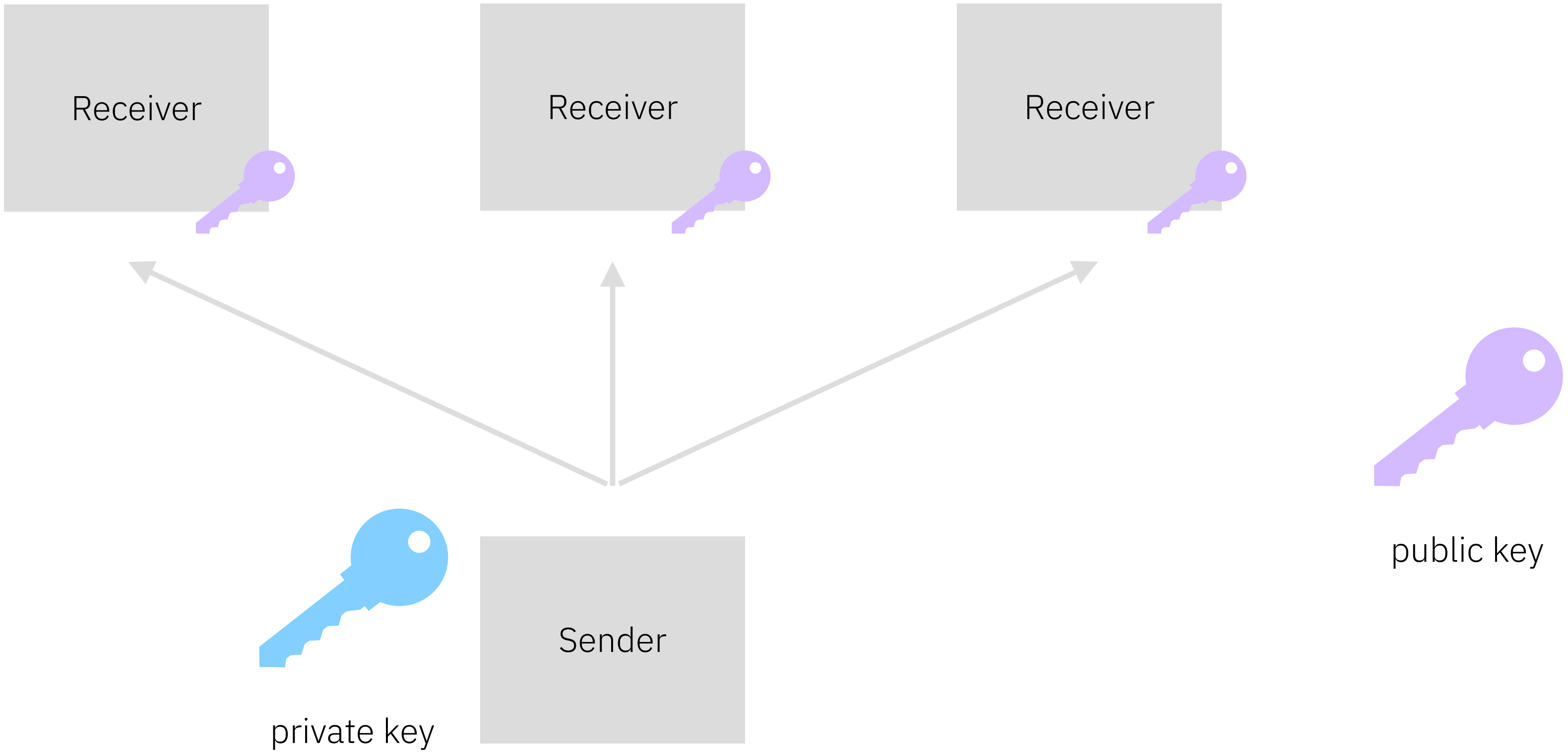
Hybrid Encryption

Asymmetric encryption computationally expensive
→ combination of symmetric and asymmetric schemes is used

This is called hybrid encryption.

1. key distribution (public key cryptography)
2. symmetric encryption

Digital Signatures



Best practices today

- Rivest–Shamir–Adleman (RSA)
- Diffie-Hellman
- Elliptic Curve Crypto (ECC)
- ...

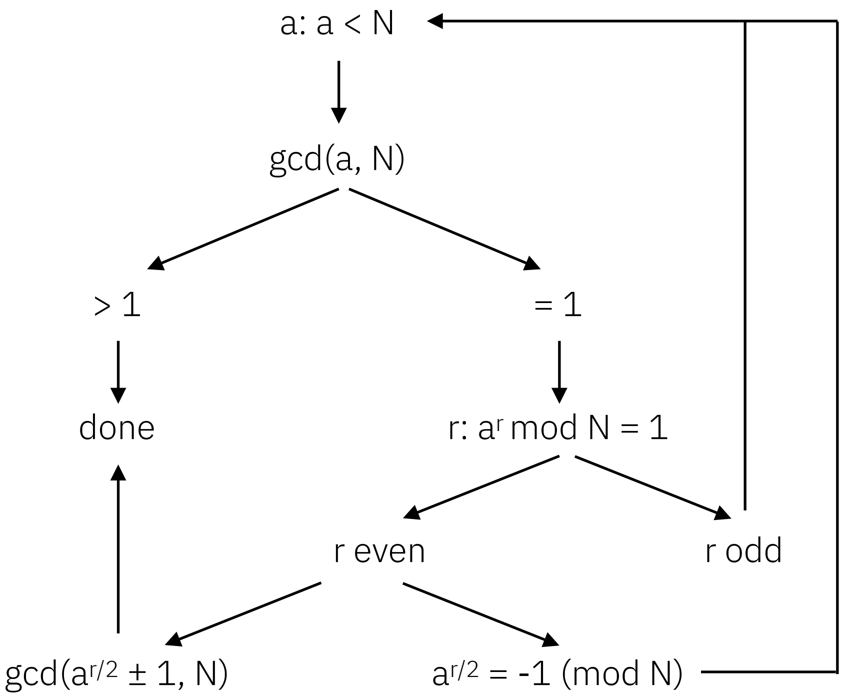
- Integer Factorization
- Discrete Logarithm
- Elliptic Curve Discrete Logarithm

1995 Peter Shor found a way to solve those problems on a quantum computer in reasonable time (polynomial in the input size).

Peter Shor
https://arxiv.org/abs/quant-ph/9508027

$$N = p \times q$$

Shor's Algorithm



Solutions

– quantum key distribution (QKD)

– quantum-safe cryptography (QSC)

Quantum Key Distribution

Exploits quantum mechanical properties to safely exchange keys. It is still an on-going research topic.

Drawbacks

– requires new hardware

– low bitrate

– range limitations

– no authentication

Quantum-safe Cryptography

Some classical algorithms are still hard for quantum computers to solve. Some of them are ready to use.

Advantages

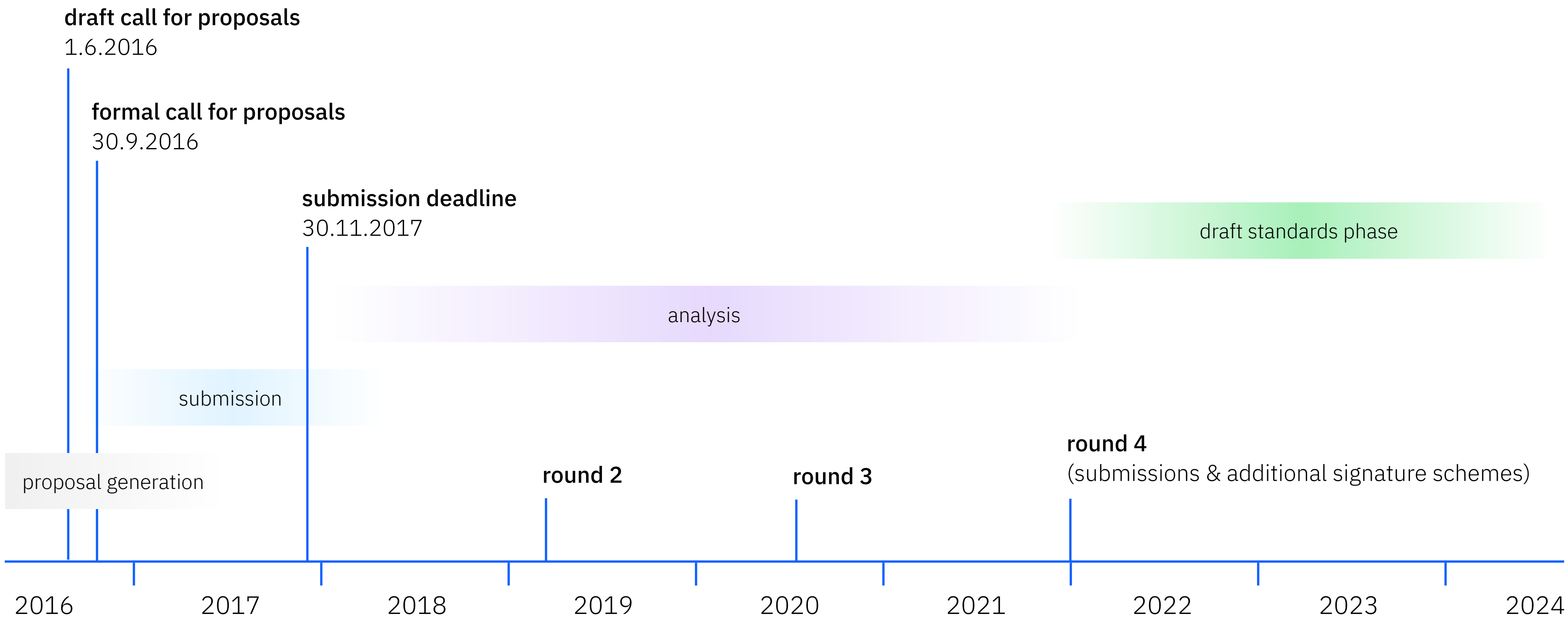
– available today

– authentication

– (almost) no new hardware necessary

Harvest now, decrypt later.

NIST Standardization Timeline



Governmental Guidance

National Institute of Standards and Technology (NIST)

- Critical to begin planning for the replacement of hardware, software, and services that use public-key algorithms now
- Be ready to adopt and implement the new algorithms at the end of the standardization process
- 5 to 15 or more years following, standardization to replace most of the vulnerable public-key systems currently in use

Bundesamt für Sicherheit in der Informationstechnik (BSI)

- The protection of long-lasting secrets makes it urgent that actions be taken now or as soon as possible
- BSI is not waiting for NIST to come out with a standard to issue technical guidance
- In high security applications, hybrid schemes (use of classical algorithms in conjunction with quantum-safe algorithms) are required by BSI

Crypto-agility!

discover & classify data

- value of data
- locations
- compliance & requirements
- data inventory with defined ownership

crypto inventory

- how your data is encrypted today
- cryptographic inventory containing certificates, encryption protocols, key lengths, ...
- inventory management, e.g. certificate lifecycle, timespan of keys, ...

crypto agility

- time to replace or update cryptography
- different dimensions of crypto agility
- testing one's crypto agility

quantum-safeness

- implementing quantum-safe algorithms
- performance impact

Quantum-safe & quantum-unsafe algorithms

type	algorithm	best practice today	quantum-safe
asymmetric	RSA	yes	no
asymmetric	ECDSA, ECDH	yes	no
asymmetric	DHE	yes	no
symmetric	DES	no	no
symmetric	AES	yes	yes
hash	SHA1	no	no
hash	MD5	no	no
hash	SHA256	yes	yes
hash	SHA3	yes	yes

Key lengths

algorithm	key length in bits	security level classical computer in bits	security level in quantum computer in bits
RSA public key encryption	1024	80	broken
	2048	120	broken
elliptic curve cryptography	256	128	broken
	384	192	broken
AES	128	128	64
	256	256	128

NIST Standardization Candidates

key exchange

– Classic McEliece (Code), IBMer participating

– CRYSTALS–Kyber (Lattice), IBM

– NTRU (Lattice)

– SABER (Lattice)

signatures

– CRYSTALS–Dilithium (Lattice), IBM

– FALCON (Lattice), IBM

– Rainbow (Multivariate)

Quantum-safe features on IBM z15

- SHA & AES natively supported
- SMF records since z/OS 2.4 second quantum-safe signature (Cryptographic Support for z/OS V2R2 – V2R4 with APAR OA57371)
- ICSF (with CEX7S enabled)
  - Enterprise Public-Key Cryptography Standards #11 (PKCS#11)
  - IBM Common Cryptographic Architecture (CCA)

Fast Quantum-Safe Cryptography on IBM Z

Jonathan Bradbury[1] and Basil Hess[2]

[1] IBM Systems, Poughkeepsie, USA
[2] IBM Research Europe, Rueschlikon, Switzerland

Abstract. Performance of software implementations on today's available hardware architectures plays a crucial role in the adoption of quantum-safe cryptography. An important target for quantum-safety are IBM Z® systems, which run and secure a majority of all worldwide transactions. With its current z15 architecture, the platform offers a range of ISA extensions suitable for optimizing quantum-safe algorithms. In this work, we present optimizations of two promising candidates in the third round of the NIST PQC standardization process: SIKE and Dilithium. Our SIKE implementation covers NIST security levels 1-5. It uses vectorization techniques for its $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ arithmetic and achieves a significant speedup compared to generic implementations, running in 3.4 ms (encaps + decaps) for NIST level 1. Our Dilithium implementation benefits from vector optimizations applied to NTT and to sampling, and from SHA3 instructions on z15, running in 42.8 µs (sign) and 14.7 µs (verify) for NIST level 2. We present insights on the z15 ISA, on the implementations, evaluation results and provide an outlook of further optimization potential.

Keywords: Quantum Safe, IBM Z, SIKE, Dilithium, Optimization, Evaluation

SIKE Results

Performance (in thousands of cycles) of SIKE on an IBM z15 LPAR at 5.2 GHz. Cycle counts are rounded to the nearest 103 cycles.

SIKE in alternative candidates, good for constrained bandwidth & storage settings.

Scheme	KeyGen	Encaps	Decaps	**total** (Encaps + Decaps)
SIKEp434				
Portable C	22’771	36’807	39’089	75’897
This work	5’233 (1.01 ms)	8’676 (1.67 ms)	9’141 (1.76 ms)	17’818 (3.43 ms)
Speedup	4.4 x	4.2 x	4.3 x	4.3 x
SIKEp503				
Portable C	34’442	57’364	60’663	118’028
This work	8’200 (1.58 ms)	13’915 (2.68 ms)	14’763 (2.84 ms)	28’667 (5.51 ms)
Speedup	4.2 x	4.1 x	4.1 x	4.1 x
SIKEp610				
Portable C	61’783	113’745	114’270	228’015
This work	12’428 (2.39 ms)	23’338 (4.49 ms)	23’400 (4.50 ms)	46’738 (8.99 ms)
Speedup	5.0 x	4.9 x	4.9 x	4.9 x
SIKEp751				
Portable C	110’838	179’540	193’048	372’589
This work	21’908 (4.21 ms)	37’700 (7.25 ms)	37’560 (7.22 ms)	75’260 (14.47 ms)
Speedup	5.1 x	4.8 x	5.1 x	5.0 x

Dilithium Results

Performance (in cycles) of Dilithium on an IBM z15 LPAR at 5.2 GHz.

	KeyGen	Sign	Verify
Dilithium2			
Portable C (ref)	684’841	3’102’625	763’919
This work	104’000 (20.0 µs)	253’239 (48.7 µs)	93’080 (17.9 µs)
Speedup	6.6 x	12.3 x	8.2 x
Dilithium2-AES			
Portable C (ref)	1’241’346	3’939’394	1’231’936
This work	84’760 (16.3 µs)	222’565 (42.8 µs)	76’440 (14.7 µs)
Speedup	14.6 x	17.7 x	16.1 x
Dilithium3			
Portable C (ref)	1’213’252	5’231’388	1’217’799
This work	239’201 (46.0 µs)	419’118 (80.6 µs)	142’999 (27.5 µs)
Speedup	5.1 x	12.5 x	8.5 x
Dilithium3-AES			
Portable C (ref)	2’362’562	6’878’307	2’053’712
This work	201’238 (38.7 µs)	367’647 (70.7 µs)	112’321 (21.6 µs)
Speedup	11.7 x	18.7 x	18.3 x
Dilithium5			
Portable C (ref)	1’748’487	5’842’697	1’861’797
This work	266’762 (51.3 µs)	538’191 (103.5 µs)	234’519 (45.1 µs)
Speedup	6.6 x	10.9 x	7.9 x
Dilithium5-AES			
Portable C (ref)	3’608’605	8’163’265	3’466’667
This work	204’362 (39.3 µs)	458’109 (88.1 µs)	177’317 (34.1 µs)
Speedup	17.7 x	17.8 x	19.6 x

Color palette

Black R0 G0 B0 #000000	**Gray 100** R22 G22 B22 #161616	**Gray 90** R38 G38 B38 #262626	**Gray 80** R57 G57 B57 #393939	**Gray 70** R82 G82 B82 #525252	**Gray 60** R111 G111 G111 #6f6f6f	**Gray 50** R141 G141 B141 #8d8d8d	**Gray 40** R168 G168 B168 #a8a8a8	**Gray 30** R198 G198 B198 #c6c6c6	**Gray 20** R224 G224 B224 #e0e0e0	**Gray 10** R244 G244 B244 #f4f4f4	**White** R255 G255 B255 #ffffff
	Blue 100 R0 G17 B65 #001141	**Blue 90** R0 G29 B108 #001d6c	**Blue 80** R0 G45 B156 #002d9c	**Blue 70** R0 G67 B206 #0043ce	**Blue 60** R15 G98 B254 #0f62fe	**Cyan 50** R17 G146 B232 #1192e8	**Cyan 40** R51 G177 B255 #33b1ff	**Cyan 30** R130 G207 B255 #82cfff	**Cyan 20** R186 G230 B255 #bae6ff	**Cyan 10** R229 G246 B255 #e5f6ff	
	Red 50 R250 G77 B86 #fa4d56	**Red 40** R255 G131 B137 #ff8389	**Red 30** R255 G179 B184 #ffb3b8	**Red 20** R255 G215 B217 #ffd7d9	**Red 10** R255 G241 B241 #fff1f1	**Purple 50** R165 G110 B255 #a56eff	**Purple 40** R190 G149 B255 #be95ff	**Purple 30** R212 G187 B255 #d4bbff	**Purple 20** R232 G218 B255 #e8daff	**Purple 10** R246 G242 B255 #f6f2ff	
	Green 30 R111 G220 B140 #6fdc8c	**Green 20** R167 G240 B186 #a7f0ba	**Green 10** R222 G251 B230 #defbe6	**Yellow 20** R253 G220 B105 #fddc69	**Yellow 10** R252 G244 B214 #fcf4d6	**Teal 50** R0 G157 B154 #009d9a	**Teal 40** R8 G189 B186 #08bdba	**Teal 30** R61 G219 B217 #3ddbd9	**Teal 20** R158 G240 B240 #9ef0f0	**Teal 10** R217 G251 B251 #d9fbfb	