qsecp1024k1: An Experimental 1024-bit Koblitz-form Elliptic Curve

EVTRAPPER

evtrapper@gmail.com

Technical Specification, Validation Findings, and Deployment Requirements

Public Research Draft

22 August 2026

Abstract. qsecp1024k1 is an experimental prime-field elliptic curve for research into ultra-high classical security and transitional quantum-resource margins. It uses $y^2 = x^3 + 7$ over a 1024-bit prime field, a 1024-bit probable-prime-order group, and declared cofactor one. One motivation is to explore whether larger elliptic-curve parameters could provide an additional safeguard against an early generation of fault-tolerant quantum computers that might be capable of attacking conventional 256-bit curves but not yet have the resources to attack a 1024-bit curve. This is not a claim of post-quantum security. The accompanying source release deterministically regenerates the parameters and checks the CM relation, group order evidence, generator order, cofactor argument, nonsingularity, anomalous condition, and a bounded MOV screen. The versioned signing design uses rejection sampling, auxiliary masking, length framing, canonical encodings, and explicit point validation. Remaining blockers include portable primality certificates, complete twist analysis, fixed-width constant-time arithmetic, independent cryptanalysis, and a named external audit. The construction is nonstandard and unsuitable for production.

1. Motivation, Potential Uses, and Scope

The purpose of publishing qsecp1024k1 is to expose an unusual 1024-bit elliptic-curve design to reproducible mathematical review, implementation criticism, and public cryptanalysis. Its research questions are whether a transparent j-invariant-zero curve can sustain a classical work factor near 2^{512}, what engineering cost that entails, whether the increased quantum resources could provide a useful transitional margin, and which protocol and implementation assumptions become dominant at that scale.

1.1 Transitional quantum-resource hypothesis

The motivating hypothesis is deliberately narrower than post-quantum security. A first generation of cryptographically relevant, fault-tolerant quantum computers may have enough logical qubits, error-corrected circuit depth, and runtime to attack conventional 256-bit elliptic curves without immediately having enough resources to attack a 1024-bit curve. Published Shor resource models scale logical qubits approximately linearly with the field size and dominant gate counts approximately cubically, with architecture-dependent logarithmic factors and time-space tradeoffs. Under the 2017 Roetteler-Naehrig-Svore-Lauter model, moving from 256 to 1024 bits increases the leading logical-qubit estimate by about four and the leading Toffoli-gate estimate by roughly eighty. Later circuit work changes constants and tradeoffs but not the fact that the larger instance demands materially more fault-tolerant resources.

Accordingly, qsecp1024k1 may be described as exploring a potentially defensible transitional margin against early quantum capability. It must not be described as quantum-proof, quantum-safe, or impervious to quantum attack. Once a sufficiently scalable fault-tolerant computer exists, Shor's algorithm solves the discrete logarithm problem on both conventional and 1024-bit curves in polynomial time. The only defensible deployment concept is defense in depth alongside standardized post-quantum signatures, never in place of them.

1.2 Potential research and transitional uses

Subject to independent validation and review, possible uses include: benchmarking ultra-large prime-field elliptic-curve arithmetic; studying transparent curve generation and endomorphism-aware attack costs; evaluating a classical component in a versioned hybrid signature; testing cryptographic agility and migration procedures; and investigating whether an oversized classical component can preserve verification continuity during the earliest stage of quantum transition. These are specialized research or defense-in-depth uses, not evidence that ordinary applications require 512-bit elliptic-curve security.

Three properties must remain separate: field-element width, generic group-attack cost, and system assurance. A 1024-bit field does not by itself establish 512-bit security. The group admits automorphisms, the signature layer depends on an experimental sponge construction, and the current OpenSSL reference path is not a production constant-time implementation. The curve also provides no transaction anonymity by itself; ownership graphs, amounts, timing, and network metadata require a separate privacy protocol.

2. Domain Parameters

All integers are hexadecimal and most-significant byte first. The curve is

$$E / F_p : y^2 = x^3 + 7 \pmod{p}$$

2.1 Field prime p

```
C2E0419B6291A7D77623CB047027755E8C13FF15DF9FA77C7290F6A1197B2A41
E6431450F417A29781BC9FBB827800C44E69DA789C93430B5BC64D364062EB72
E519ACF8C844B0F2810763FF61305EE6EF84B8D6F08D2E624EC31621BD326CFF
CA4046461A6943738236EE435F3ACEEA7330EA71231808DB0BA9B911B46B07FF
```

The modulus p has 1024 bits and satisfies p mod 12 = 7. Therefore p mod 4 = 3, permitting square roots by exponentiation to (p+1)/4, and p mod 3 = 1, placing this j-invariant-zero curve in the ordinary rather than supersingular case. The coefficients are a = 0 and b = 7, and the discriminant is nonzero modulo p.

2.2 Prime group order n

```
C2E0419B6291A7D77623CB047027755E8C13FF15DF9FA77C7290F6A1197B2A41
E6431450F417A29781BC9FBB827800C44E69DA789C93430B5BC64D364062EB71
F50014C55098010EF0A092374B388F4DC1D89D2E5BD48659E0CCB13B6ABD02BC
F6A6C4C106C45BD3E545F90191253447B7C1B9F66C67879628FC9C65250CCA13
```

The declared cofactor is h = 1. The order n is slightly greater than p, with n-p having 512 bits.

2.3 Generator G

```
Gx =
16501C2F061D039789A1CD1DE46D7522907E84121DE2942353D9382B8EB0A7A6
695991F786734472DE46E826C3ED761E2BA95D8B643B7B47E4F131F7A8DE423B
BFBF66B6DF0D2E2859A496FB5E8432434B12EF7E17529190DCD7337B05015FE6
AA96218E80344AB76F311116E183EF059DD110A653E54FFA821D4DE9D6C11D0D

Gy =
9EC71B1042A06A03F110F62BF64306D3904DA0C0068184C496CF917D6668D11F
5EE0C7DBF56AA64F04D85B708E75D6893CA8AA9FE41EA614732312B1002C0939
EE1A1D572F1E0360F6F5BB3C66AEE4226E7D0D73115D3366B5B1FD44C375C83A
99BD50680FF30321CDFC0B8CD9570E0E8022EC008F4E1AA45BE2F64EE3CEED88
```

The selected G_y is even. Its compressed encoding is prefix 02 followed by the 128-byte G_x coordinate.

3. Reproducible Parameter Generation

For exact reproducibility, the complete seed and generation domain are published below as canonical ASCII octets encoded in hexadecimal. No bytes are omitted.

3.1 Canonical generation inputs

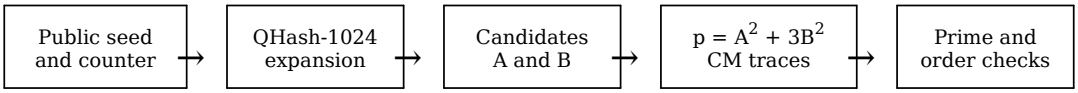
Seed octets:

```
71736563703130323 46B31206E6F7468696E672D75702D6D792D736C65657665
20736565642076312032303236 2D30382D3232
```

QHash-1024 parameter-generation domain octets:

```
71736563703130323 46B312F706172616D657465722D67656E65726174696F6E
```

The first accepted result occurs at counter 340591, CM trace candidate 5, and generator x-offset 2. The exact domain expands the seed, counter, and labels A and B. The generator forces A even and not divisible by three and B odd, then computes $p = A^2 + 3B^2$.



For the accepted counter:

```
A = 67179501E078F4B81D3AFC23FCB4E8A3175FDD8F3A6EABAAD58A423FD38C15C5
 56704F2B68D7920288404DC18633977736CD31E0FB5F49C300A514F79067C44A

B = 7265B9BC72B736DE8F35EF4EB0E43D696C5953129A62713BC12AE2620CAB2AAD
 63589AE57ED4288B61BB1656716DBB5DFB69761E90AFEE57F670BB36B54200BD
```

The selected trace is t = 3B - A and n = p + 1 - t. The six candidates are +/-2A, +/-(A+3B), and +/-(A-3B). Candidate 5 produces the accepted probable-prime order n. Conditional on primality of n, [n]G = O, G != O, and Hasse's bound placing the full curve order below 2n imply that the curve order is exactly n and the cofactor is one.

3.2 Bundled computational status

The bundled verifier reconstructs $p = A^2 + 3B^2$, t = 3B - A, n = p + 1 - t, the generator equation, [n]G = O, and the cofactor-one argument. It runs OpenSSL BN_check_prime for p and n and screens MOV embedding degrees through k = 100000. These are reproducible computations and strong probable-prime evidence, not a portable proof of primality or an independent audit. The release therefore labels formal primality certificates and independent order verification as unresolved publication requirements.

4. QHash-1024 Specification

QHash-1024-v1 is a domain-separated sponge over the 24-round Keccak-f[1600] permutation. It is not SHA-3, SHAKE, or a FIPS-approved named construction. Its parameters are rate r = 576 bits (72 bytes), capacity c = 1024 bits, and output length 1024 bits (128 bytes). The capacity and output support a generic collision target of 2^{512}, assuming the standard sponge model and no structural attack on the full permutation.

4.1 Byte-level algorithm

Initialize the 1600-bit state to zero and position to zero. Absorb, in order: the fixed prefix octets below; the domain length as a two-byte unsigned little-endian integer; the exact domain octets; and the message octets. Absorption XORs each octet into the rate portion in little-endian 64-bit lane order and applies Keccak-f[1600] whenever the 72-byte rate is full. Finalization XORs suffix 1F at the current rate position and 80 at the final rate byte, applies the permutation, then squeezes 128 bytes from the rate portion, applying another permutation after each 72 output bytes.

Fixed prefix octets:

```
51534543502D514841534831303234 2D5631
```

The domain length must be at most 65535 bytes. All callers must treat the domain as protocol data, not a display label. Any change to the prefix, domain encoding, suffix, rate, capacity, output length, or lane order defines a different function.

4.2 Known-answer vectors

For domain ASCII `qsecp1024k1/specification/KAT`, the 128-byte outputs are:

Empty message:

```
fc3c6cc920b38a0a891fc40b12589c986092c033453d1346ca78e2ece90a7326
5613cdece6975871442f7316f64bbd0d98da1123a6cc3f78adf70686c61f35ef
b49c9a9ad7fa83e12636de0f88fde21296a89b0b0111026f047fcf6e2812f261
e9eed7e2994f1fbb6ffac27e63ba017a94a029be464ed67ad841f394c4846db7
```

Message ASCII abc:

```
779a642b91d5bc29e5ea26e48053efb0510d50bb453862d2bd40f29e0dcb6af6
b2bf8c9d7375728e566985417eaf06a2ef275e6ea719179a884cc04b9368bd3b
17e3a1ac5084a2a2e7ef3e8c590b866f4f449f33c404f3dde29a23fa5df9d1a9
b7b29cd54554f9e8ee019e3e9dc520afbba5ade067b179e13a1754973f11a5c7
```

4.3 Security interpretation

A 512-bit digest such as SHA-512 has a generic 256-bit collision bound, but this does not prove that every Schnorr signature using it is automatically limited to 256-bit EUF-CMA security. Reusing an observed signature on a second message requires a second preimage under the fixed R.x and P.x transcript. An arbitrary birthday collision chosen before the signer produces R is not, by itself, an immediate forgery. Separately, any prehash or transaction-identifier layer may be collision-limited and must be analyzed in its actual protocol context.

5. Encodings and Canonical Validation

Curve integers use fixed-width big-endian encoding. Implementations must keep field elements modulo p and scalars modulo n as distinct types. They must never parse s as a field element or silently reduce a noncanonical input.

Object	**Encoding**
Secret scalar	128 bytes
X-only public key	128 bytes
Compressed public key	129 bytes
Uncompressed public key	257 bytes
QSchnorr1024 signature	256 bytes (R.x || s)
QHash-1024 digest	128 bytes

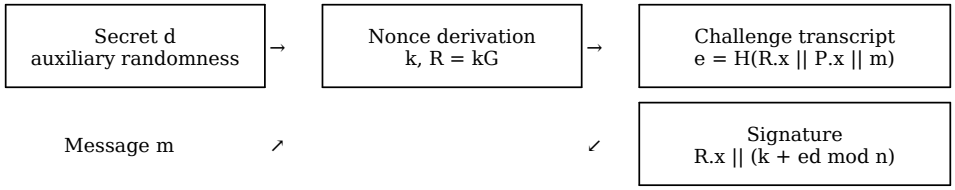
Verification must reject P.x >= p, R.x >= p, or s >= n before curve arithmetic. Approximately 38.2 percent of uniformly random 128-byte strings exceed either modulus, so these checks are routine rather than rare edge cases. Since n > p, a mathematically valid scalar can satisfy p <= s < n and must remain a scalar. The interval has relative size about $2^{-511.39}$; the claim that a malicious signer can force such a valid signature on demand is not established. Nevertheless, a fixed known-answer test in this interval is required to prevent implementations from confusing the two moduli.

5.1 Parameter checksums

Object	**SHA-256 of canonical big-endian octets**
p	0d2d9e999e8eff6468430d1ea0d336ec5265d1072db32c164e0477498657bd8f
n	d12f76707708bf906947007331080b33288591f16d40fb7ad4d1845e5b5d23ea
Gx	9f8177170e11fe0d59aeb8b9f3698bf942feb6367df08e66ec0f0cd95a1ecb54
Gy	18eca137cf3b4ef22eb74ff43e8d7e71b521ec576b34069bc6120e11a9810c04
A	550b9654b09b655e13e31a661791abce3918bb6ad8dac33c015c88d57a3f09c1
B	13bc3cb3cf91ce3ceeef9a64d6e1bb9cb77d8271e55e4bd2506fcfdb47c6efed
twist order	a3fe1788f295181c56451069e0d6a370186f5ba7dcf522a2e200f3a50938e12d

6. QSchnorr1024-v1 and Unbiased Scalar Derivation

QSchnorr1024-v1 is inspired by BIP340 but is deliberately distinct. Its curve, widths, domains, auxiliary construction, and hash function differ. An earlier prototype reduced a single 1024-bit digest directly modulo n, which produced a substantial scalar-distribution bias. Version 1 does not use that conversion: every nonce and challenge scalar is obtained by deterministic rejection sampling under new versioned domains.



6.1 Rejected prototype conversion

For a uniform 1024-bit digest X, direct reduction X mod n would make residues below 2^{1024}-n occur twice as often as the remaining residues. The total variation distance from uniform is approximately 0.145912. The Shannon entropy loss relative to a uniform scalar is approximately 0.06970 bits and the min-entropy loss is approximately 0.30581 bits. This rejected construction is documented so implementers do not reproduce it; signatures made with it are outside version 1.

6.2 Normative unbiased conversion

Version 1 uses deterministic rejection sampling. For counter i = 0, 1, 2, ... encode i as four-byte unsigned big-endian, compute QHash-1024(domain, transcript || i), decode the 128-byte output as a big-endian integer x, and accept only when 0 < x < n for private keys and nonces, or 0 <= x < n for challenges. Otherwise increment i. The expected number of attempts is approximately 1.62. The counter and rejection behavior are protocol-critical and are covered by bundled versioned known-answer vectors.

The exact version 1 nonce-domain and challenge-domain octets are published below. They are distinct from all earlier experimental transcripts.

```
nonce domain: 7173656370313032346B312F515363686E6F7272313032342D76312F6E6F6E6365
challenge domain: 717365637031303234 6B312F515363686E6F7272313032342D76312F6368616C6C656E6765
```

6.3 Transcript and edge requirements

Version 1 defines auxiliary-randomness masking, eight-byte big-endian message-length framing, exact domain octets, secret and nonce normalization, retry counters, and canonical failure behavior. Verification performs the range checks of Section 5 and rejects any public x-coordinate that does not lift to the required even-y point. Batch verification is intentionally outside version 1 and requires a separate specification before use.

7. Security Analysis

7.1 Generic group strength and endomorphisms

Pollard rho is proportional to sqrt(n), suggesting a nominal 2^{512} scale. Here log2(n) is approximately 1023.606. The j-invariant-zero form admits a six-element automorphism group. Applying a sqrt(6) automorphism speedup and the usual sqrt(pi/4) factor gives an estimated generic work factor of approximately $2^{510.34}$ group operations. This is an attack-model estimate, not a security proof. A strict target above 2^{512} would require a larger order and fresh parameter generation.

7.2 Transfer attacks

The curve is not anomalous and is not supersingular. The bundled verifier checks p^k != 1 mod n for every k <= 100000. This is strong evidence against a low-degree MOV reduction but is not a proof of the full embedding degree. An independent implementation should repeat and extend the bound before any production consideration.

7.3 Quadratic twist

The quadratic-twist order is

```
C2E0419B6291A7D77623CB047027755E8C13FF15DF9FA77C7290F6A1197B2A41
E6431450F417A29781BC9FBB827800C44E69DA789C93430B5BC64D364062EB73
D533452C3FF160D6116E35C777282E801D30D47F8545D66ABCB97B080FA7D742
9DD9C7CB2E0E2B131F27E3852D50698D2EA01AEBD9C88A1FEE56D5BE43C945ED
```

The exact partial factorization established by the bundled verifier and resumed search is:

```
3 * 277 * 1264261 * 37009471 * 52879243 *
14707268336212449843888 1 *
150092599233416885671815302629 69 * C230
```

C230 is the following unresolved 230-decimal-digit, 763-bit composite:

```
30151351756120053776928987876119423592925247878052365616231457904419961386075128322029202698905689775614006084886 34
40082822092575185604682883295460843796206262532835867325919037930778151688055069420779050919392571966315492753103 87
```

The seven listed factors passed 128-round OpenSSL probable-prime tests. Their 262-bit product is

```
45386549453317080678747333232821247009737436066068926672849734342618432104172 47
```

and multiplication by C230 exactly reproduces the published twist order. C230 remained unresolved after the configured P-1, P+1, and ECM p35 through p40 searches. This is not a complete twist factorization and does not establish twist security. It does not break the probable-prime-order main group; full point validation rejects ordinary twist inputs. The factors remain relevant to defense in depth against omitted validation, x-only arithmetic, faults, and future protocol paths.

7.4 Constant-time and fault resistance

The OpenSSL EC_GROUP and BIGNUM reference path sets constant-time flags on secret scalars, serializes the shared BN_CTX, obtains private randomness from RAND_priv_bytes, and cleanses temporary secret buffers. These are defensive improvements, not a platform-wide constant-time guarantee. Production work still requires a dedicated fixed-width field and scalar implementation, complete or carefully unified formulas, scalar blinding where appropriate, fault checks, and empirical dudect, ctgrind, and TVLA testing. QSchnorr's lack of modular inversion during signing and verification is useful but does not resolve the remaining side-channel surfaces.

7.5 Classical versus quantum security

Shor's algorithm applies regardless of the larger parameters. The larger field can raise the logical-qubit, circuit-depth, gate-count, error-correction, and runtime requirements, so a machine able to attack a conventional curve is not automatically able to attack qsecp1024k1 at the same moment. That creates a plausible transitional resource margin, not a new hardness assumption. Resource ratios cannot be converted into a defensible calendar prediction such as months or one hardware generation without a physical architecture, logical error rate, code distance, clock rate, routing model, and parallelization strategy. Long-term quantum resistance requires a standardized post-quantum signature or a carefully specified hybrid combiner.

8. Standards and Strategic Context

Custom elliptic curves are outside the approved algorithm paths used for FIPS 140-3 and U.S. National Security Systems. NIST's standardized quantum-resistant signatures are ML-DSA and SLH-DSA. NSA's December 2024 CNSA 2.0 FAQ specifies ML-DSA-87 for digital signatures, requires compliant new NSS acquisitions by 2027, phases out incompatible equipment by the end of 2030, and mandates CNSA 2.0 algorithms by the end of 2031. This curve should therefore be presented as a research artifact, not as a procurement substitute for standardized cryptography.

The main practical comparison is not between 128-bit and 512-bit classical attack labels in isolation. Existing 128-bit classical security is already beyond plausible brute force, while this design imposes substantially larger keys, signatures, bandwidth, implementation complexity, and unoptimized arithmetic cost. Its proposed value is the combination of transparent experimentation, an unusually large classical margin, and the possibility of buying additional time against an early resource-limited quantum adversary when used beside standardized post-quantum cryptography. It is not an assertion that current systems generally require 512-bit elliptic-curve security.

9. Conclusion

qsecp1024k1 has internally consistent domain arithmetic supported by bundled reproducibility checks: a 1024-bit probable-prime field, a 1024-bit probable-prime order, conditional cofactor-one reasoning, a verified generator, and an estimated generic attack cost near $2^{510.34}$. QHash-1024 is specified as a 1024-bit-capacity Keccak-f[1600] sponge, making a 512-bit generic collision target plausible under the sponge model rather than proven for the complete protocol.

QSchnorr1024-v1 removes the earlier scalar bias through versioned rejection sampling and adds transcript framing, auxiliary masking, canonical validation, secret cleanup, and committed vectors. The twist remains only partially factored, the OpenSSL path is not a production constant-time foundation, and no independent audit or portable primality certificates are bundled. No real-value deployment is recommended. The curve remains classical, nonstandard, and separate from any transaction-privacy design. Its quantum-related claim is limited to a possible transitional resource margin against early fault-tolerant machines, not resistance to a mature cryptographically relevant quantum computer.

References

[1] Bertoni, Daemen, Peeters, and Van Assche, The Sponge and Duplex Constructions, including the capacity-based generic security model. https://keccak.team/sponge_duplex.html.

[2] NIST, FIPS 186-5: Digital Signature Standard, Appendix A.4; and SP 800-186: Recommendations for Discrete Logarithm-Based Cryptography. FIPS 186-5; SP 800-186.

[3] Roetteler, Naehrig, Svore, and Lauter, Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms, ASIACRYPT 2017; Haener, Jaques, Naehrig, Roetteler, and Soeken, Improved Quantum Circuits for Elliptic Curve Discrete Logarithms, 2020; NIST, FIPS 204 and FIPS 205; NSA, CNSA 2.0 FAQ, version 2.1, December 2024. 2017 resource estimates; 2020 circuit improvements; FIPS 204; FIPS 205; CNSA 2.0 FAQ.