CRYPTOGRAPHY AND ALGEBRAIC APPLICATIONS, INVERTIBILITY OF EXPONENTIATION MAPS AND SECURITY ASSUMPTIONS

Xilola Qobil-qizi Yaxshilikova
yaxshilikovaxilola1004@gmail.com
JDPU

Abstract: This article examines the algebraic correctness of RSA, Diffie-Hellman, and elliptic-curve key-agreement mechanisms separately from their security assumptions. The aim is to delineate the logical boundaries between the invertibility of exponentiation maps, the equality of shared values, and resistance to attacks. The investigation is based on theoretical proofs, counterexamples that violate the requisite conditions, and exhaustive enumeration of finite models. For RSA, a bijectivity criterion for exponentiation modulo a product of distinct primes is established using the Chinese remainder theorem. It is shown that violating the exponent condition causes distinct messages to map to the same value, whereas, when the modulus is not squarefree, a condition imposed on the group of units is insufficient for all messages. Computational checks examined 143 RSA messages, 100 pairs of exponents in a prime-order Diffie-Hellman subgroup, 361 additions in an elliptic-curve group, and 6,859 associativity instances. No discrepancies were observed in models with valid parameters; with an invalid RSA exponent, only 18 distinct ciphertexts were produced. The results explicitly distinguish algebraic correctness conditions from security requirements. The contribution of this work consists in combining established algebraic results with positive and negative computational checks; no new cryptosystem is proposed. Computations with small parameters do not assess practical security. The conclusions substantiate the independent importance of authentication, standardized encoding, and key derivation.

Keywords: RSA; modular arithmetic; bijection; cyclic group; Diffie-Hellman; elliptic curve; computational verification

1 Introduction

In public-key cryptography, the efficiency of legitimate computation and the difficulty of the inverse problem without secret information are distinct requirements [1-3]. A proof of successful decryption or agreement between keys cannot be substituted for a security proof. This study addresses the question: which algebraic conditions ensure the correctness of a mechanism, and what specific failure occurs when those conditions are violated? To this end, a necessary and sufficient criterion for RSA, a group invariant for key agreement, and positive and negative checks of these properties are considered together.

2 Materials and Methods

The study is theoretical, analytical, and computational in nature. The original constructions [1-3] were compared with algebraic references [4, 5] and official specifications [6-11]. Sources were selected on the basis of their direct relevance to the claims under examination; this work is not a systematic literature review. Computations were performed using exact integer arithmetic in Python 3.12.14. The results of fast modular exponentiation were independently checked by repeated multiplication, while modular inverses were verified using the Euclidean algorithm and exhaustive enumeration. No timing or performance benchmarks were conducted.

2.1 Algebraic Domain and Notation

$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ denotes the ring of residue classes; the notation $a \equiv b \pmod{n}$ means that $n \mid (a - b)$. Its group of units is denoted by $\mathbb{Z}_n^{\times}$. An element a has a multiplicative inverse if and only if

$\gcd(a,n) = 1$: the extended Euclidean algorithm yields the identity $au + nv = 1$, and hence $a^{-1} \equiv u \pmod{n}$. For a prime p, $\mathbb{Z}_p = \mathbb{F}_p$ is a field. Throughout, p and q are distinct primes, $n = pq$, and e is a positive integer exponent [4, 5].

3 Results

3.1 Bijectivity Criterion for RSA

Proposition 1. The map $T_e: \mathbb{Z}_n \to \mathbb{Z}_n$, $T_e(m) = m^e$ is bijective if and only if

$$\gcd\big(e, \lambda(n)\big) = 1, \qquad \lambda(n) = \operatorname{lcm}(p-1, q-1). \tag{1}$$

This is a statement of the classical criterion for a squarefree modulus in the form relevant to the present analysis [2, 5]. Proof**.** By the Chinese remainder theorem,

$$\mathbb{Z}_n \cong \mathbb{F}_p \times \mathbb{F}_q. \tag{2}$$

In each field, zero maps to itself, while the nonzero elements form cyclic groups of orders $p - 1$ and $q - 1$, respectively. In a cyclic group of order h, exponentiation corresponds to multiplication of exponents by e; it is a permutation precisely when $\gcd(e, h) = 1$. Thus, bijectivity of both components is equivalent to the stated criterion.

When the criterion holds, a positive exponent d is chosen such that $ed \equiv 1 \pmod{\lambda(n)}$. If $p \mid m$, then $m^{ed} \equiv m \equiv 0 \pmod{p}$; if $p \nmid m$, Fermat's theorem gives $m^{ed} \equiv m \pmod{p}$. The same argument applies to q. Consequently,

$$c \equiv m^e \pmod{n} \quad \Rightarrow \quad c^d \equiv m \pmod{n}. \tag{3}$$

The proof covers all messages; a message need not be coprime to the modulus. Direct application of Euler's theorem, by contrast, is restricted to the group of units.

3.2 RSA Verification Example and Counterexamples

For $p = 11$, $q = 13$, and $n = 143$, we have $\lambda(n) = 60$. Choosing $e = 7$ and $d = 43$ gives $ed = 301 = 5 \cdot 60 + 1$. The encryption of the message $m = 42$ by repeated squaring is:

$$42^2 \equiv 48, \quad 42^4 \equiv 16, \quad 42^7 \equiv 81 \pmod{143}. \tag{4}$$

Since $43 = 32 + 8 + 2 + 1$,

$$81^2 \equiv 126, \quad 81^8 \equiv 9, \quad 81^{32} \equiv 126 \pmod{143}, \tag{5}$$

$$81^{43} \equiv 126 \cdot 9 \cdot 126 \cdot 81 \equiv 42 \pmod{143}. \tag{6}$$

An independent check gave $81^{43} \equiv 9 \pmod{11}$ and $81^{43} \equiv 3 \pmod{13}$; the value 42 has these same residues. For the zero divisor $m = 13$, one likewise obtains $13^7 \equiv 117$ and $117^{43} \equiv 13 \pmod{143}$. Figure 1 illustrates verification of the computation modulo the two primes.

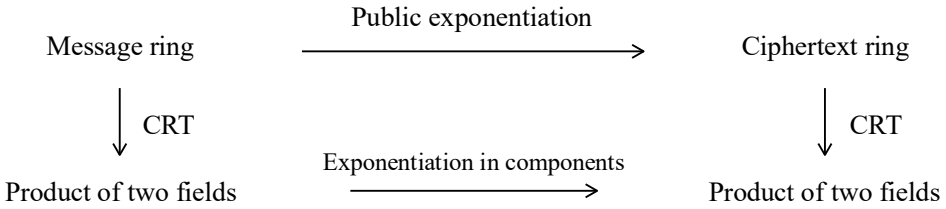


Figure 1. Diagram for verifying the RSA computation via the Chinese remainder theorem. Both paths yield the same residue class; the diagram was prepared on the basis of [2, 5].

Negative control. For the same modulus, setting $e = 6$ gives $1 + \frac{10}{\gcd(6,10)} = 6$ and $1 + \frac{12}{\gcd(6,12)} = 3$ distinct images in the two fields, respectively; only 18 distinct ciphertexts remain in total. Consequently, the map has no single-valued inverse function. Squarefreeness also matters: for $n = 9$ and $e = d = 5$, one has $ed \equiv 1 \pmod{6}$, but $3^{25} \equiv 0 \not\equiv 3 \pmod{9}$.

3.3 Diffie-Hellman in a Prime-Order Subgroup

Let $G = \langle g \rangle$ be a cyclic group of order r, with secret exponents $a, b \in \{1, \dots, r-1\}$. For the public elements $A = g^a$ and $B = g^b$,

$$K_A = B^a = g^{ab} = A^b = K_B. \quad (7)$$

In the example, $p = 23$, $g = 2$, and $r = 11$: $2^{11} \equiv 1 \pmod{23}$, $2 \not\equiv 1 \pmod{23}$, and 11 is prime. Choosing $a = 6$ and $b = 7$ gives $A = 18$, $B = 13$, and $13^6 \equiv 18^7 \equiv 6 \pmod{23}$. An independent calculation yields $2^{42} \equiv 2^9 \equiv 6 \pmod{23}$. This equality does not authenticate the participants [1, 8].

3.4 Conditions for a Well-Defined Elliptic Curve

For a prime $p > 3$ and $\alpha, \beta \in \mathbb{F}_p$,

$$E\colon y^2 = x^3 + \alpha x + \beta, \qquad 4\alpha^3 + 27\beta^2 \not\equiv 0 \pmod{p}. \quad (8)$$

$E(\mathbb{F}_p)$ is an abelian group consisting of the affine solutions and the identity element $\mathcal{O}$ [3, 4]. For $P = (x_1, y_1)$, $Q = (x_2, y_2)$, and $x_1 \neq x_2$, the addition formulas over the field are:

$$s = \frac{y_2 - y_1}{x_2 - x_1}, \qquad x_3 = s^2 - x_1 - x_2, \qquad y_3 = s(x_1 - x_3) - y_1. \quad (9)$$

Division means multiplication by the modular inverse of the denominator. If $P = Q$ and $y_1 \neq 0$, then $s = \frac{3x_1^2 + \alpha}{2y_1}$. For $Q = -P$, $P + Q = \mathcal{O}$; when $y_1 = 0$, $2P = \mathcal{O}$. Moreover, $P + \mathcal{O} = P$. Special cases are handled before any division is performed.

The verification model was defined by $p = 17$, $\alpha = \beta = 2$, and $P = (5,1)$. Nonsingularity is verified by $140 \equiv 4 \pmod{17}$, and point membership by $1^2 \equiv 5^3 + 2 \cdot 5 + 2 \pmod{17}$. In the doubling computation, $2^{-1} \equiv 9 \pmod{17}$, and

$$s \equiv 77 \cdot 9 \equiv 13, \quad x_3 \equiv 6, \quad y_3 \equiv 3 \pmod{17}. \quad (10)$$

Thus, $Q = 2P = (6,3)$. In the next addition, $s = 2$, giving $R = P + Q = (10,6)$. Direct substitution yields $3^2 \equiv 6^3 + 2 \cdot 6 + 2 \equiv 9 \pmod{17}$ and $6^2 \equiv 10^3 + 2 \cdot 10 + 2 \equiv 2 \pmod{17}$. A reverse check was performed using $R + (-P) = Q$: $s \equiv 15 \pmod{17}$, with the result $(6,3)$.

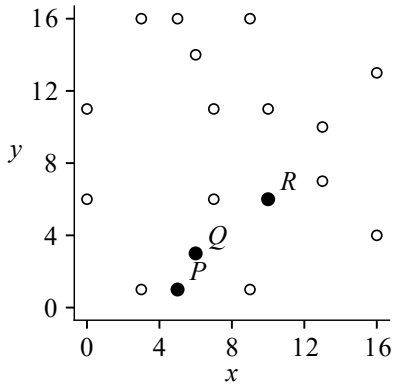


Figure 2. All affine points of the verification curve over a finite field. The labeled points are the results of the additions discussed in the text; the identity element is not represented in the plane. The plot was prepared from the computed coordinates.

3.5 Agreement Between Exhaustive Enumeration and Algebraic Results

In the elliptic-curve model, every coordinate pair was substituted into the equation, yielding 18 affine points; including the identity element, the group has order 19. By Lagrange's theorem and the primality of the group order, the order of P is also 19. Repeated addition confirmed $19P = \mathcal{O}$. Closure was checked for every pair, and associativity for every triple. The checks reported in Table 1 exhaust the specified domains; the results are not a statistical sample.

Table 1.

Results of computational verification using exact arithmetic

Verification object	Verification domain	Result
RSA decryption	$0 \le m < 143; e = 7, d = 43$	143 cases; 0 errors
RSA negative control	$0 \le m < 143; e = 6$	18 distinct images
DH shared value	$1 \le a, b \le 10$	100 pairs; 0 discrepancies
Elliptic-curve addition	$E(\mathbb{F}_{17})^2$	361 pairs; closure preserved
Elliptic-curve associativity	$E(\mathbb{F}_{17})^3$	6859 triples; 0 discrepancies

The numerical result of the RSA negative control agrees exactly with the theoretical calculation of the cardinality of the image. This agreement provides a stronger check than a single successful example: the verification procedure is also sensitive to violations of the condition. However, enumeration in a finite group does not replace the general associativity theorem.

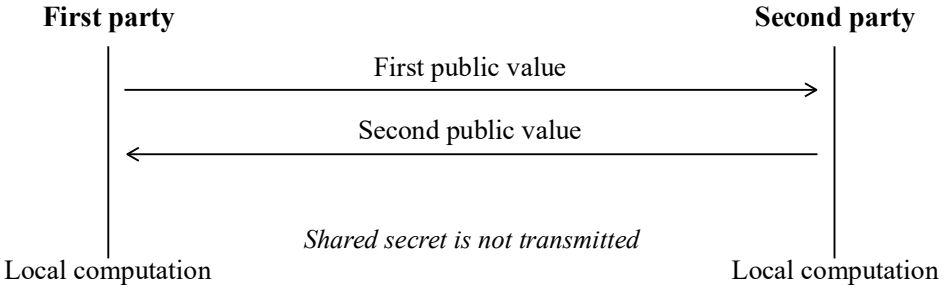


Figure 3. Separation of public exchange and local computation in Diffie-Hellman. The transmitted values are public; the shared secret value is not sent over the channel. The diagram was prepared on the basis of [1, 8].

4 Discussion

4.1 The Boundary Between Correctness and Security

The protocol in Figure 3 can be subject to a man-in-the-middle attack even though equality of the shared values is maintained: an active attacker establishes separate agreements with each party. Thus, the invariant is not a substitute for authentication. Likewise, RSA bijectivity does not guarantee confidentiality for deterministic textbook RSA. Practical encryption requires an encoding scheme such as RSAES-OAEP, whereas signatures use a separate construction such as RSASSA-PSS [7]. The shared DH element is not itself a ready-to-use symmetric key either: a suitable key-derivation function, such as HKDF, is applied [10].

4.2 Computational Problems and Parameters

Table 2 distinguishes the basis for correctness from the problem an attacker must solve. Factoring the RSA modulus suffices to recover the secret exponent, but no general equivalence between RSA inversion and factoring is assumed. The discrete logarithm problem (DLP) concerns recovering the exponent, whereas computational Diffie-Hellman (CDH) concerns computing the shared element from two public powers. ECDLP and the computational ECDH problem are their counterparts in an elliptic-curve group [4, 7, 8].

Table 2.

Difference between an algebraic invariant and a computational assumption

Mechanism	Basis of correctness	Separate security problem
RSA	CRT and exponentiation permutation	RSA inversion; factoring is sufficient
Diffie-Hellman	Laws of exponents	CDH; DLP solves it

Mechanism	Basis of correctness	Separate security problem
Elliptic-curve DH	Consistency of scalar operations	Elliptic-curve CDH; ECDLP solves it

In NIST's correspondence for classical 128-bit security, the RSA modulus is specified as 3072 bits, the finite-field DH modulus as 3072 bits and its subgroup order as 256 bits, and the elliptic-curve subgroup order as ranging from 256 to 383 bits [6]. These are not the sizes of entire key files. For an exponent or scalar of length ℓ bits, binary methods require $O(\ell)$ corresponding group operations. Because the bit costs of these operations differ, this does not imply a direct speed advantage. In a generic prime-order group, the expected work of Pollard's rho method is $O(\sqrt{r})$ group operations [4].

Using the same algebraic domain does not imply relying on the same security assumption. For example, AES uses arithmetic in $\mathbb{F}_{2^8}$, but it does not conceal a discrete logarithm [11]. Modulo $f(t) = t^8 + t^4 + t^3 + t + 1$, the identity $t \cdot t^7 \equiv t^4 + t^3 + t + 1 \pmod{f(t)}$ illustrates byte arithmetic.

Shor's algorithm solves factoring and discrete logarithms in polynomial time in the quantum model [12]. Therefore, conformity with classical parameter recommendations does not imply quantum resistance. FIPS 203, 204, and 205 specify ML-KEM, ML-DSA, and SLH-DSA, respectively; these constructions rely on different computational foundations [13-15]. Side channels, random-number generators, and practical encoding implementations were not tested in this study.

5 Conclusion

A bijectivity criterion for RSA was established for all residue classes, and negative controls demonstrated the necessity of the conditions on the exponent and the structure of the modulus. In the prime-order DH subgroup and the elliptic-curve group, the invariants agreed with the results of exhaustive enumeration. This agreement verifies the internal consistency of the algebraic model, not practical security. The scope of the scientific contribution is the integration of established theorems into a verifiable comparative framework; no new theorem on resistance to attack is claimed. The next stage requires validation with standardized parameters and independent implementations, as well as a separate investigation of side-channel risks.

References

[1] Diffie W., Hellman M. E. New directions in cryptography. IEEE Transactions on Information Theory. 1976;22(6):644–654. https://doi.org/10.1109/TIT.1976.1055638

[2] Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. 1978;21(2):120–126. https://doi.org/10.1145/359340.359342

[3] Miller V. S. Use of Elliptic Curves in Cryptography. In: Williams H. C., ed. Advances in Cryptology — CRYPTO '85 Proceedings. LNCS 218. Springer; 1986:417–426. https://doi.org/10.1007/3-540-39799-X_31

[4] Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. CRC Press; 1996. https://cacr.uwaterloo.ca/hac/

[5] Shoup V. A Computational Introduction to Number Theory and Algebra. 2nd ed. Cambridge University Press; 2008. https://www.shoup.net/ntb/

[6] Barker E. Recommendation for Key Management: Part 1 — General. NIST SP 800-57 Part 1 Rev. 5. 2020. https://doi.org/10.6028/NIST.SP.800-57pt1r5

[7] Moriarty K., Kaliski B., Jonsson J., Rusch A. PKCS #1: RSA Cryptography Specifications Version 2.2. RFC 8017. 2016. https://doi.org/10.17487/RFC8017

[8] Barker E., Chen L., Roginsky A., Vassilev A., Davis R. Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. NIST SP 800-56A Rev. 3. 2018. https://doi.org/10.6028/NIST.SP.800-56Ar3

[9] Langley A., Hamburg M., Turner S. Elliptic Curves for Security. RFC 7748. 2016. https://doi.org/10.17487/RFC7748

[10] Krawczyk H., Eronen P. HMAC-based Extract-and-Expand Key Derivation Function (HKDF). RFC 5869. 2010. https://doi.org/10.17487/RFC5869

[11] National Institute of Standards and Technology. Advanced Encryption Standard (AES). FIPS 197. 2001; updated 2023. https://doi.org/10.6028/NIST.FIPS.197-upd1

[12] Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing. 1997;26(5):1484–1509. https://doi.org/10.1137/S0097539795293172

[13] National Institute of Standards and Technology. Module-Lattice-Based Key-Encapsulation Mechanism Standard. FIPS 203. 2024. https://doi.org/10.6028/NIST.FIPS.203

[14] National Institute of Standards and Technology. Module-Lattice-Based Digital Signature Standard. FIPS 204. 2024. https://doi.org/10.6028/NIST.FIPS.204

[15] National Institute of Standards and Technology. Stateless Hash-Based Digital Signature Standard. FIPS 205. 2024. https://doi.org/10.6028/NIST.FIPS.205