RSAC 2026 Conference

POWER OF COMMUNITY.

SoK: A Generalized Attack on RSA and Its Variants

Mengce Zheng

Associate Professor
Zhejiang Wanli University

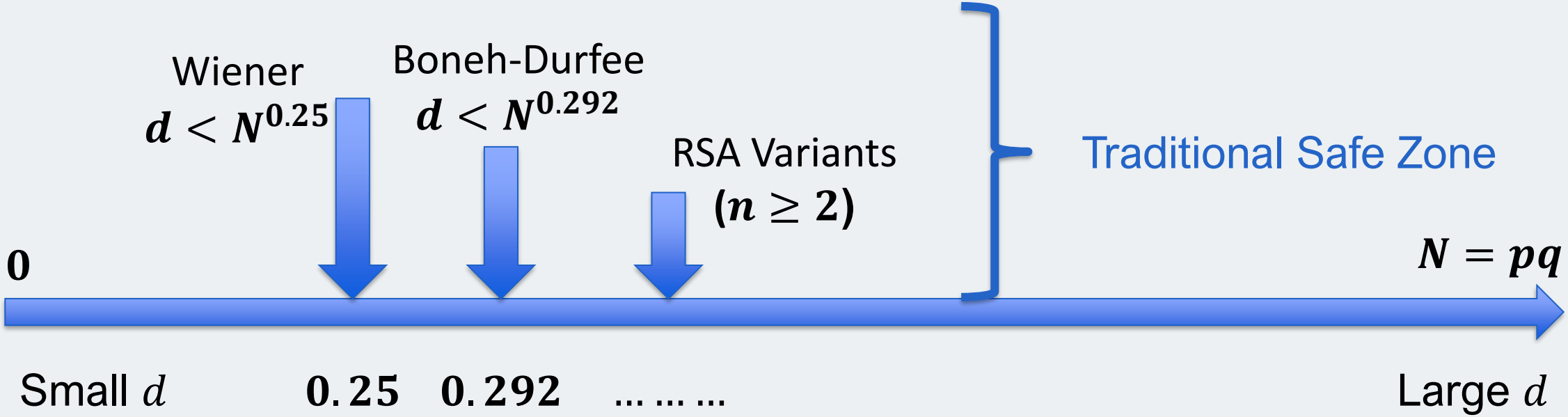
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC (“RSAC”) or any other co-sponsors. RSAC does not endorse or approve, and assumes no responsibility for, the content, accuracy, or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio, and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2026 RSA Conference LLC. All rights reserved.

The Status of RSA Security

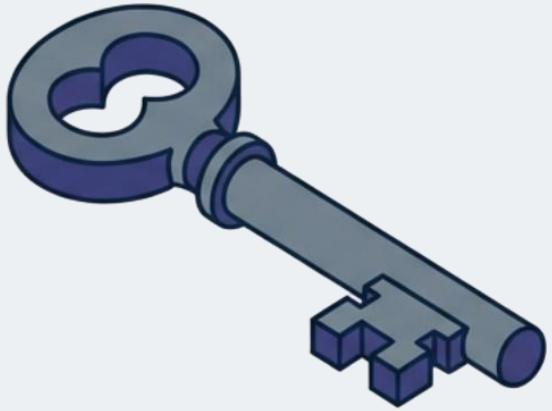


$$ed \equiv 1 \bmod \varphi(N) \Rightarrow ed \equiv 1 \bmod (p-1)(q-1)$$

Current Cryptanalysis: A large private key d ensures security.

Blind Spot: Is Size the Only Vulnerability?

Standard View

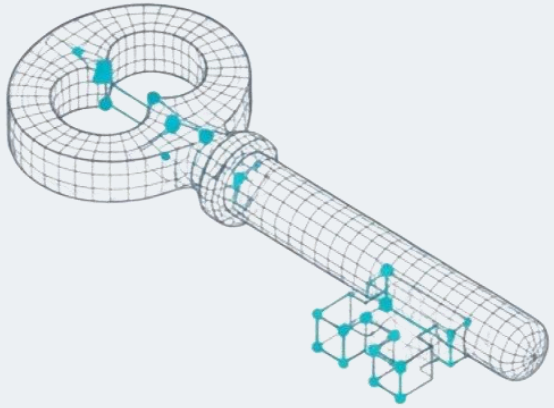


Large d $(d \approx N)$

Could RSA be weak even if d is large and theoretically safe from all known attacks?

Yes!

Generalized View



Hidden Algebraic Perturbations

Redefining RSA's Modular Structure

Standard RSA

$$\varphi(N) = (p-1)(q-1)$$

Known RSA Variants

$$\psi_n(N) = (p^n - 1)(q^n - 1)$$

New Generalized Key Equation

$$\psi_n(N, a, b) = (p^n - a)(q^n - b)$$

Crucial Insight

Traditional functions are merely special instances where $a = b = 1$. By allowing a and b to vary, there exists a massive, previously invisible attack surface.

The Generalized Key Equation

Public Exponent (Known)

Generalized Inverse (Replacing d)

$$eu \equiv 1 \bmod \psi_n(N, a, b)$$

Hidden Structure $(p^n - a)(q^n - b)$

Paradigm Shift: No longer hunting for d, but hunting for u, the inverse with respect to a perturbed structure defined by unknown a and b.

One Framework to Rule Them All

Attack / Research	Fixed Parameters	Insecure Bound (δ)
Boneh-Durfee	$n = 1, a = 1, b = 1$	$\delta < 1 - \sqrt{2}/2 \approx 0.292$
Peng et al. / Zheng et al.	$n = 2, a = 1, b = 1$	$\delta < 2 - \sqrt{\alpha}$
Teleseanu	arbitrary $n, a = 1, b = 1$	$\delta < n - \sqrt{\alpha n/2}$
Our Generalized Attack	arbitrary n, unknown $a, b \geq 1$	**New Attack Surface**

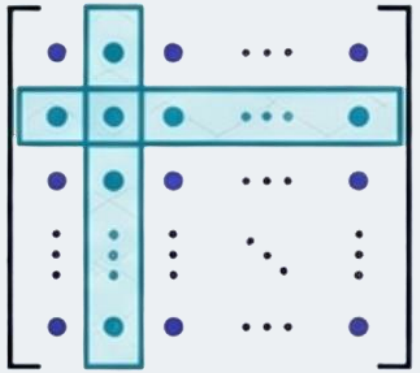
Note: Previous research only explored a single line for $a = b = 1$!

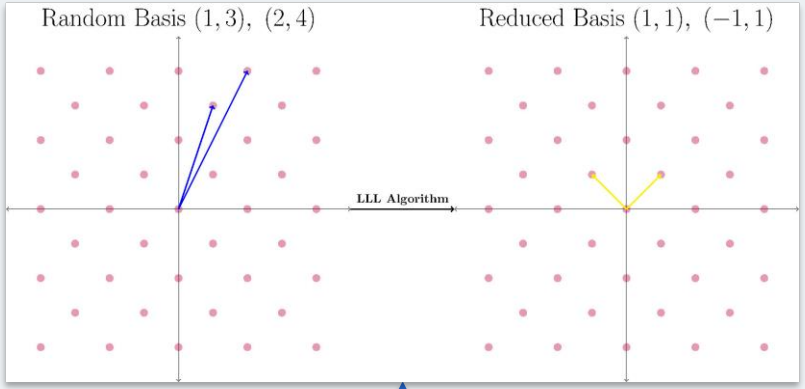
Attack Engine: Coppersmith & Lattices

Target Polynomial → Linearization → Lattice → LLL Reduction

$$eu \equiv 1 \bmod \psi_n(N, a, b)$$
$$\Downarrow$$
$$f(x, y) = x(N^n + y) + 1 \bmod e$$

Herrmann-May technique reduces to the linear form $g(x, z)$ using $z = xy + 1$





RSAC 2026 Conference

From Approximations to Exact Factors

LLL Output Small Roots

$$y_0 = -(aq^n + bp^n - ab)$$

$$p, q$$

Error term: $|aq^n - bp^n| < 2N^{n/2}$

New Technique: Lemma 1

Step 1: Recover Sum S & Difference D

$$S = aq^n + bp^n \text{ and } D = |aq^n - bp^n|$$

Step 2: Extract Two Primes p & q

$$p, q = \{\gcd(N, S + D), \gcd(N, S - D)\}$$

New Bounds of Vulnerability

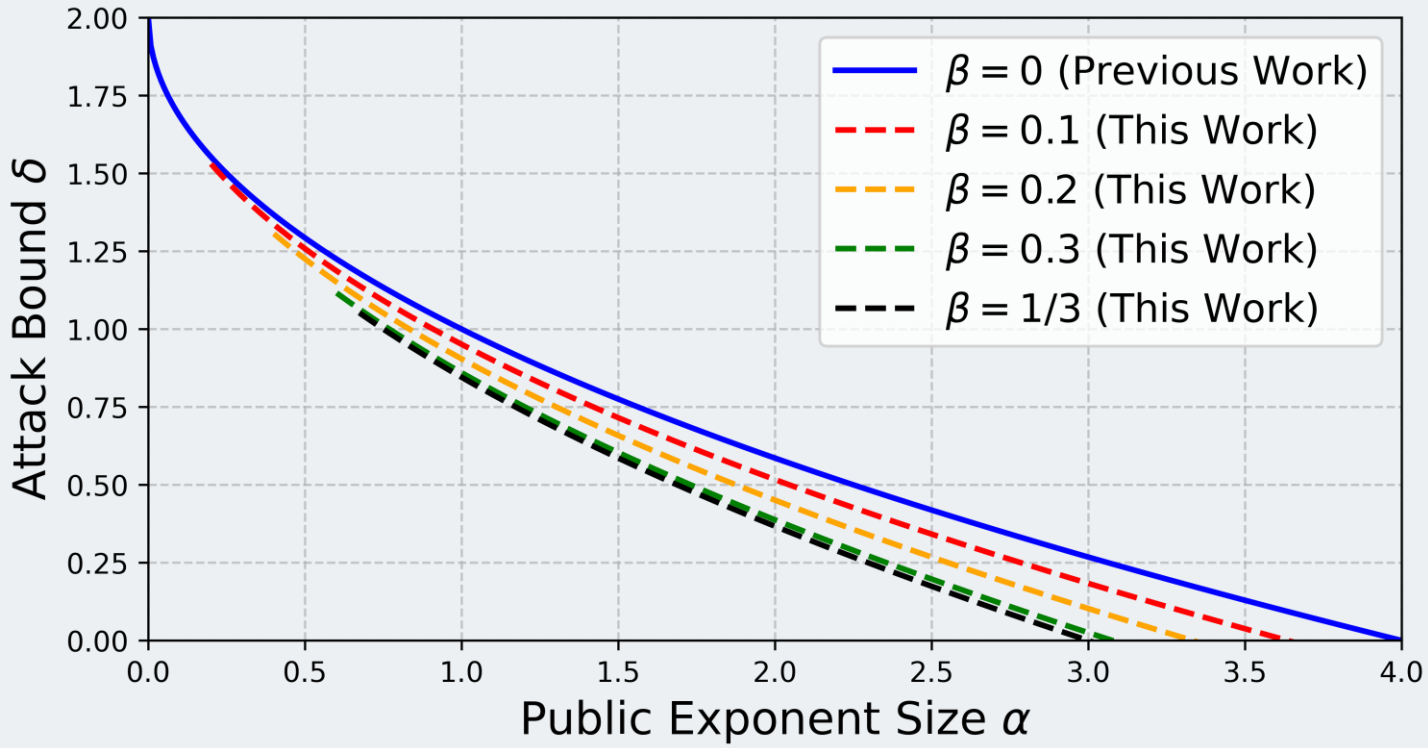
$$\delta < n - \frac{\sqrt{\alpha(2\beta + n)}}{2}$$

- α: Size of Public Key ($e = N^{\alpha}$)
- β: Size of Structural Perturbation ($a, b \leq N^{\beta}$)
- δ: Size of Generalized Inverse ($u < N^{\delta}$)

Constraint: The attack holds if parameters satisfy this bound, provided that

$$\alpha > n/2 + \beta \text{ and } \beta < n/6.$$

Visualizing the Attack Surface (2D)

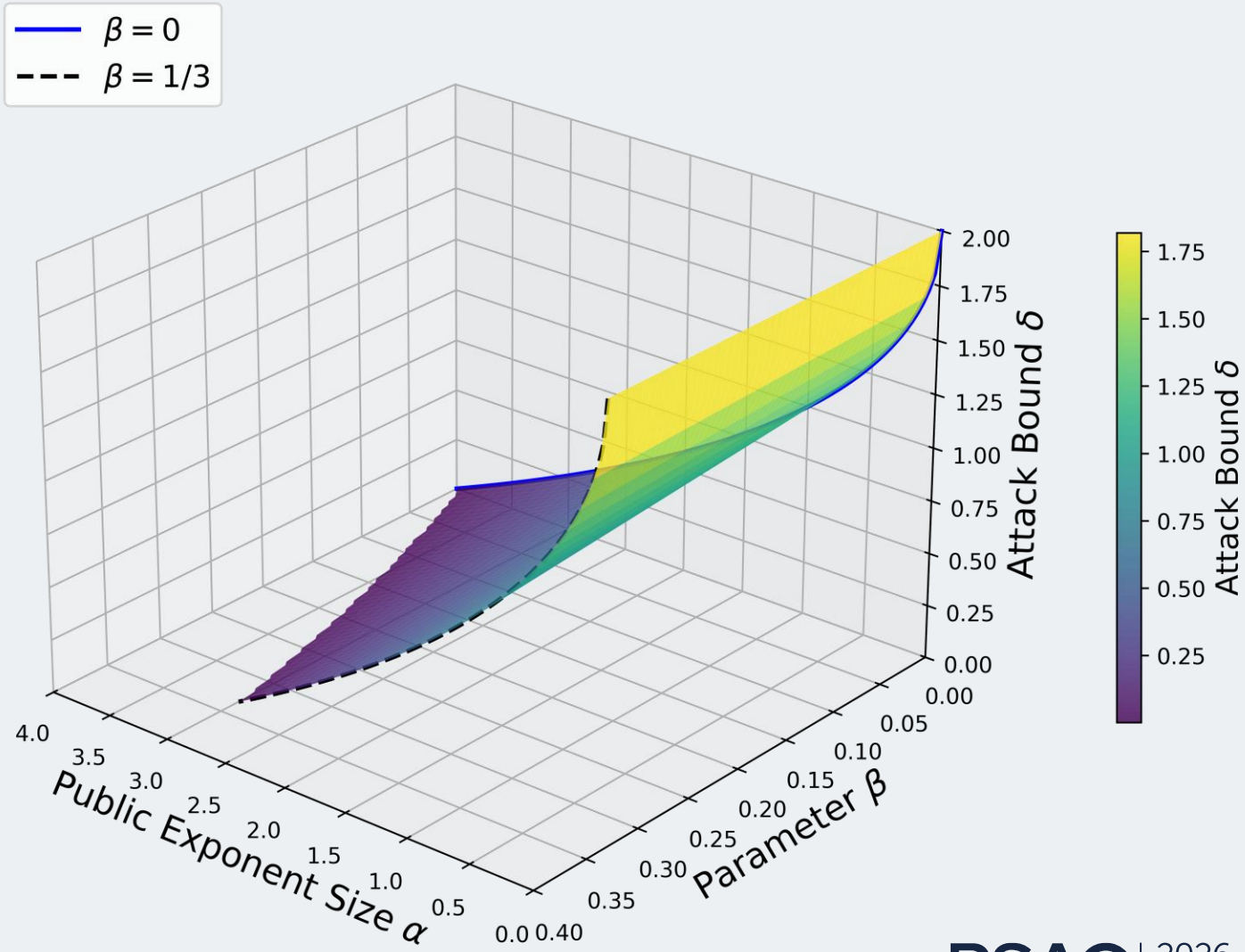


Note: Increasing structural complexity lowers the curve, but reveals a multi-dimensional attack surface previously thought secure.

Visualizing the Attack Surface (3D)

Security Polytope

Security is not a binary switch; it is now a continuous geometric volume.



‘Safe’ Keys That Are Not Safe

The Illusion of Safety

- Modulus: 200-bit N and $n = 2$
- Public Key: 400-bit e ($\alpha \approx 1.988$)
- Target Private Exponent: $d \approx N^{0.988}$

Verdict: Secure against Boneh-Durfee attack and other cryptanalyses.

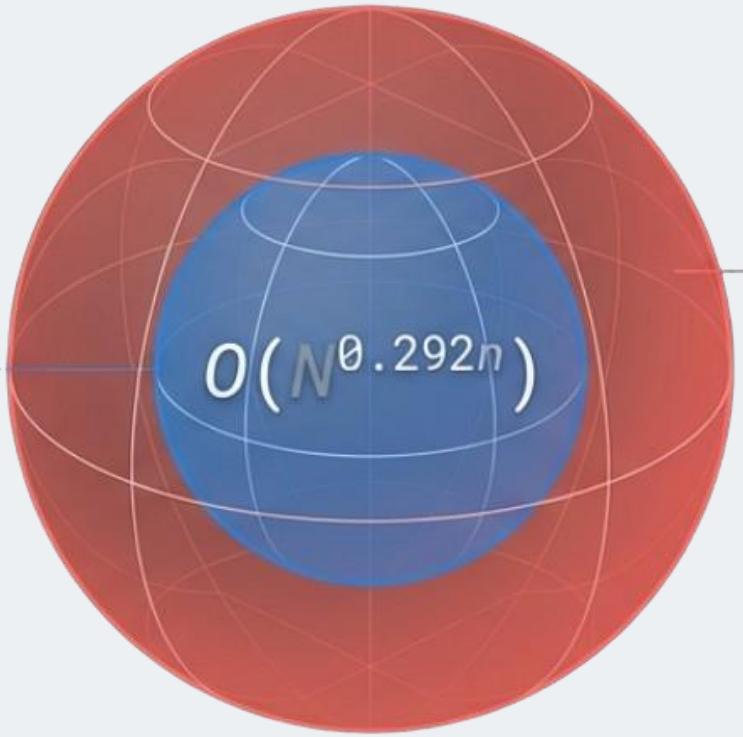
The Reality of Weakness

- Attack Parameters: $\beta = 0.25$ (unknown a, b exist)
- Generalized Inverse: $\delta = 0.35$

Result: Factoring algorithm recovers p and q in seconds.

Expanding the Weak Key Universe

Standard Weak Keys
$\mathcal{O}(N^{0.292n})$



Generalized Weak Keys
$\mathcal{O}(N^{0.350n})$

Note: An RSA instance secure against all previous attacks may still be broken if its public key possesses such hidden algebraic structure.

Apply What Have Learned

- **Analyze** existing public keys. Check for hidden algebraic relations

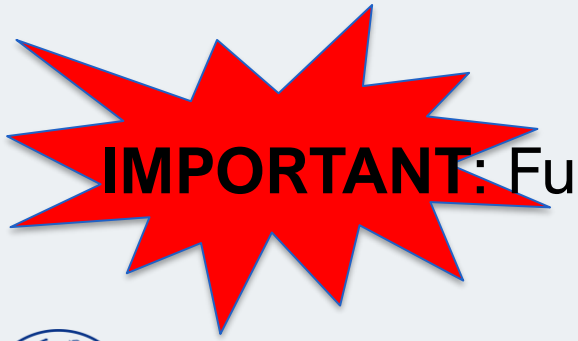
$$eu \equiv 1 \bmod \psi_n(N, a, b).$$

- **Audit** key generation libraries. Ensure entropy sources do not inadvertently create relations with small a and b.
- **Test** some keys using the open-source SageMath implementation provided

https://github.com/MengceZheng/RSA_GAF

Summary of Findings

- **Unified:** Bridged the gap between separate attacks on RSA and its variants into one algebraic framework.
- **Expansive:** Proved that several large private exponents offer no guarantee of safety if hidden structural parameters exist.
- **Constructive:** The proposed attack is practical, using LLL reduction and Lemma 1 to recover prime factors in polynomial time.



Full-size private keys are no longer assumed to ensure security!

RSAC | 2026 Conference

Thank you!

For more information:

mengce.zheng@gmail.com

POWER OF COMMUNITY.