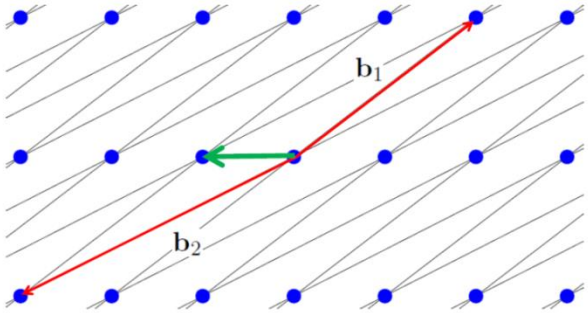


Small CRT-exponent RSA Revisited

Atsushi Takayasu（The University of Tokyo, AIST）

Yao Lu (The University of Tokyo)

Liqiang Peng (Chinese Academy of Sciences)

ePrint 2017/092

RSA

pk: $(N = pq, e)$ sk: (p, q, d)

$$ed = 1 \bmod (p-1)(q-1)$$

✓ [BD00] proposed a polynomial time factoring algorithm for

$$d < N^{0.292}$$

using lattice-based Coppersmith's method.

CRT-RSA

pk: $(N = pq, e)$ sk: (p, q, d_p, d_q)

$$ed_p = 1 \bmod (p-1), \qquad ed_q = 1 \bmod (q-1)$$

✓ Are there analogous attacks to factorize N when d_p, d_q are small?

Small d_q Attack

- p is significantly smaller than q and d_q is significantly smaller than q.
- [May@Crypto'02]

$$p < N^{0.382}$$

- [Bleichenbacher-May@PKC'06]

$$p < N^{0.468}$$

Small d_q Attack

- p is significantly smaller than q and d_q is significantly smaller than q.
- [May@Crypto'02]

$$p < N^{0.382}$$

- [Bleichenbacher-May@PKC'06]

$$p < N^{0.468}$$

- ✓ Extensions for RSA variants: [SIK@IEICE Trans.'11],[PHL+@Indocrypt'15]
- ✓ Other settings: [BM@Crypto'03],[LZL@ACNS'14], [TK@ACNS'15] ,[TK@ISC'16]

Small d_q Attack

- p is significantly smaller than q and d_q is significantly smaller than q.
- [May@Crypto'02]

$$p < N^{0.382}$$

- [Bleichenbacher-May@PKC'06]

$$p < N^{0.468}$$

Can we reach $p < N^{0.5}$?

✓ Extensions for RSA variants: [SIK@IEICE Trans.'11],[PHL+@Indocrypt'15]

✓ Other settings: [BM@Crypto'03],[LZL@ACNS'14], [TK@ACNS'15] ,[TK@ISC'16]

Small d_p, d_q Attack

- Both d_p and d_q are significantly smaller than p, q.
- [Jochemsz-May@Crypto'07]

$$\underline{d_p, d_q < N^{0.073}}$$

Small d_p, d_q Attack

- Both d_p and d_q are significantly smaller than p, q.
- [Jochemsz-May@Crypto'07]

$$\underline{d_p, d_q < N^{0.073}}$$

✓ Other settings: [SM@ACNS'09],[TK@ACNS'15]

Small d_p, d_q Attack

- Both d_p and d_q are significantly smaller than p, q.
- [Jochemsz-May@Crypto'07]

$$d_p, d_q < N^{0.073}$$

- Other settings: [SM@ACNS'09],[TK@ACNS'15]

Can we recover larger d_p, d_q?

Our Results

- Small d_q attack

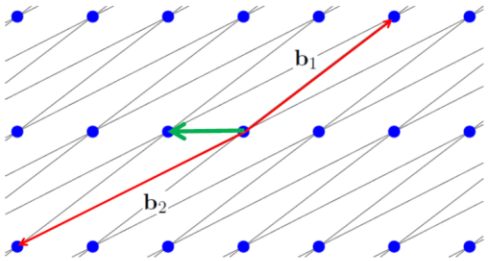
$$p < N^{0.5}$$

- Small d_p, d_q attack

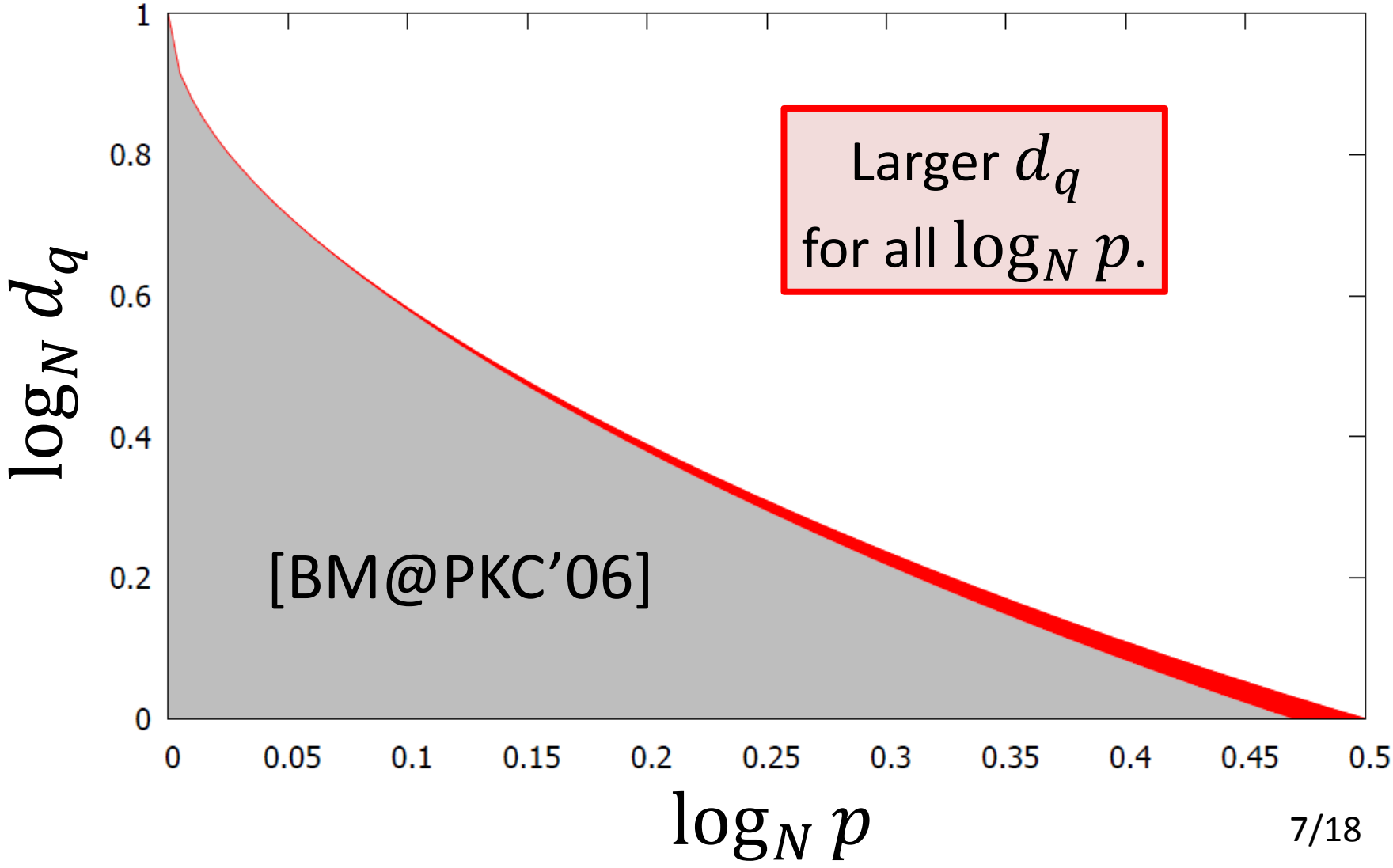
$$d_p, d_q < N^{0.122}$$

- Improved attacks on variants of CRT-RSA

✓ An improved lattice construction that is specialized to CRT-RSA key generation.



Attack Comparison



Coppersmith's Method [Cop@EC'96]

Modular equation

$$f(x, y) = 0 \mod e$$

s.t. $|\tilde{x}| < X, |\tilde{y}| < Y$

Coppersmith's Method [Cop@EC'96]

Modular equation

$$f(x, y) = 0 \mod e$$

s.t. $|\tilde{x}| < X, |\tilde{y}| < Y$

- Produce $g_1(x, y), \ldots, g_n(x, y)$ who have the same root $(x, y) = (\tilde{x}, \tilde{y})$ modulo e^m.

Coppersmith's Method [Cop@EC'96]

Modular equation

$$f(x, y) = 0 \mod e$$

s.t. $|\tilde{x}| < X, |\tilde{y}| < Y$

- Produce $g_1(x, y), \ldots, g_n(x, y)$ who have the same root $(x, y) = (\tilde{x}, \tilde{y})$ modulo e^m.
- Each row of a matrix B consists of coefficient vectors of $g_1(xX, yY), \ldots, g_n(xX, yY)$.

Coppersmith's Method [Cop@EC'96]

Modular equation

$$f(x, y) = 0 \mod e$$

s.t. $|\tilde{x}| < X, |\tilde{y}| < Y$

- Produce $g_1(x, y), \ldots, g_n(x, y)$ who have the same root $(x, y) = (\tilde{x}, \tilde{y})$ modulo e^m.
- Each row of a matrix B consists of coefficient vectors of $g_1(xX, yY), \ldots, g_n(xX, yY)$.
- If

$$|\det(B)|^{\frac{1}{n}} < e^m,$$

$(\tilde{x}, \tilde{y})$ can be recovered under heuristic assumption.

Coppersmith's Method [Cop@EC'96]

Modular equation

$$f(x, y) = 0 \mod e$$

s.t. $|\tilde{x}| < X, |\tilde{y}| < Y$

- Produce $g_1(x, y), \ldots, g_n(x, y)$ root $(x, y) = (\tilde{x}, \tilde{y})$ modulo e

How to produce B that minimizes the LSH?

- Each row of a matrix B consists of coefficient vectors of $g_1(xX, yY), \ldots, g_n(xX, yY)$.
- If

$$|\det(B)|^{\frac{1}{n}} < e^m,$$

$(\tilde{x}, \tilde{y})$ can be recovered under heuristic assumption.

Formulation

- Key generation: $ed_q = 1 + k\,(q-1)$

  $\rightarrow f_q(x_q, y_q) = 1 + x_q(y_q - 1) = 0 \mod e$

  Solution: $(x_q, y_q) = (k, q)$

Formulation

- Key generation: $ed_q = 1 + k\,(q-1)$

  $\rightarrow f_q(x_q, y_q) = 1 + x_q(y_q - 1) = 0 \mod e$

  Solution: $(x_q, y_q) = (k, q)$

- Multiplying p:

  $ed_q p = p + k\,(N-p) = N + (k-1)(N-p)$

  $\underline{\rightarrow f_p\,(x_p, y_p) = N + x_p(N - y_p) = 0 \mod e}$

  Solution: $(x_p, y_p) = (k-1, p)$

Formulation

- Key generation: $ed_q = 1 + k\,(q-1)$

  $\rightarrow f_q(x_q, y_q) = 1 + x_q(y_q - 1) = 0 \mod e$

  Solution: $(x_q, y_q) = (k, q)$

- Multiplying p:

  $ed_q p = p + k\,(N-p) = N + (k-1)(N-p)$

  $\rightarrow f_p\,(x_p, y_p) = N + x_p(N - y_p) = 0 \mod e$

  Solution: $(x_p, y_p) = (k-1, p)$

✓ Solving $f_p(x_p, y_p) = 0$ seems more appropriate since p is smaller than q.

[May@Crypto'02]'s Matrix

$$f_p(x_p, y_p) = N + x_p(N - y_p)$$

$$\begin{pmatrix}
e & & & & & & \\
0 & eX_p & & & & & \\
N & NX_p & -X_pY_p & & & & \\
0 & 0 & 0 & eY_p & & & \\
0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & & \\
0 & 0 & 0 & 0 & 0 & eY_p^2 & \\
0 & 0 & 0 & 0 & NX_pY_p^2 & NY_p^2 & -X_pY_p^3
\end{pmatrix}$$

[May@Crypto'02]'s Matrix

$$\begin{pmatrix}
e & & & & & & \\
0 & eX_p & & & & & \\
N & NX_p & -X_pY_p & & & & \\
0 & 0 & 0 & eY_p & & & \\
0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & & \\
0 & 0 & 0 & 0 & 0 & eY_p^2 & \\
0 & 0 & 0 & 0 & NX_pY_p^2 & NY_p^2 & -X_pY_p^3
\end{pmatrix}$$

Natural construction that follows [JM@AC'06].

$$|\det(B)| = e^4 X_p^4 Y_p^9$$

[May@Crypto'02]'s Matrix

$$\begin{pmatrix}
e & & & & & & \\
0 & eX_p & & & & & \\
N & NX_p & -X_pY_p & & & & \\
0 & 0 & 0 & eY_p & & & \\
0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & & \\
0 & 0 & 0 & 0 & 0 & eY_p^2 & \\
0 & 0 & 0 & 0 & NX_pY_p^2 & NY_p^2 & -X_pY_p^3
\end{pmatrix}$$

[BM@PKC'06]'s Matrix

$$
\begin{pmatrix}
e & & & & & \\
0 & eX_p & & & & \\
N & NX_p & -X_pY_p & & & \\
0 & 0 & 0 & eY_p & & \\
0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & \\
0 & 0 & 0 & 0 & 0 & eY_q \\
0 & -X_p & 0 & 0 & 0 & Y_q \quad X_pY_q
\end{pmatrix}
$$

[BM@PKC'06]'s Matrix

$$
\begin{pmatrix}
e & & & & & \\
0 & eX_p & & & & \\
N & NX_p & -X_pY_p & & & \\
0 & 0 & 0 & eY_p & & \\
0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & \\
0 & 0 & 0 & 0 & 0 & eY_q \\
0 & -X_p & 0 & 0 & 0 & Y_q \quad X_pY_q
\end{pmatrix}
$$

New varible $y_q = q$ which are not in $f_p(x_p, y_p)$; $y_p y_q = N$.

[BM@PKC'06]'s Matrix

$$\begin{pmatrix}
e & & & & & \\
0 & eX_p & & & & \\
N & NX_p & -X_pY_p & & & \\
0 & 0 & 0 & eY_p & & \\
0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & \\
0 & 0 & 0 & 0 & 0 & eY_q \\
0 & -X_p & 0 & 0 & 0 & Y_q \quad X_pY_q
\end{pmatrix}$$

[DN@AC'00]'s technique
Reducing powers of Y_p.

$$|\det(B)| = e^4 X_p^4 Y_p^9$$

$$\downarrow$$

$$|\det(B)| = e^4 X_p^4 Y_p^4 Y_q^2$$

[BM@PKC'06]'s Matrix

$$\begin{pmatrix}
e & & & & & & \\
0 & eX_p & & & & & \\
N & NX_p & -X_pY_p & & & & \\
0 & 0 & 0 & eY_p & & & \\
0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & & \\
0 & 0 & 0 & 0 & 0 & eY_q & \\
0 & -X_p & 0 & 0 & 0 & Y_q & X_pY_q
\end{pmatrix}$$

Either y_p or y_q appeared in every monomial.

Observation

- [May@Crypto'02]
  Solve $f_p(x_p, y_p) = 0$ since p is smaller than q.

- [Bleichenbacher-May@PKC'06]
  Reducing the determinant with a new variable q.

Observation

- [May@Crypto'02]
  Solve $f_p(x_p, y_p) = 0$ since p is smaller than q.
  $\rightarrow p < N^{0.5}$ seems infeasible.
- [Bleichenbacher-May@PKC'06]
  Reducing the determinant with a new variable q.
  $\rightarrow$ Should we follow [May@Crypto'02]'s approach?

Observation

- [May@Crypto'02]
  Solve $f_p(x_p, y_p) = 0$ since p is smaller than q.
  $\rightarrow p < N^{0.5}$ seems infeasible.
- [Bleichenbacher-May@PKC'06]
  Reducing the determinant with a new variable q.
  → Should we follow [May@Crypto'02]'s approach?

➢ We solve simultaneous modular equations

$$f_p(x_p, y_p) = 0, \qquad f_q(x_q, y_q) = 0.$$

[BM@PKC'06]'s Matrix

$$
\begin{pmatrix}
e & & & & & \\
0 & eX_p & & & & \\
N & NX_p & -X_pY_p & & & \\
0 & 0 & 0 & eY_p & & \\
0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & \\
0 & 0 & 0 & 0 & 0 & eY_q \\
0 & -X_p & 0 & 0 & 0 & Y_q \quad X_pY_q
\end{pmatrix}
$$

[BM@PKC'06]'s Matrix

$$
\begin{pmatrix}
e & & & & & & \\
0 & eX_p & & & & & \\
N & NX_p & -X_pY_p & & & & \\
0 & 0 & 0 & eY_p & & & \\
0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & & \\
 & & & & & & \\
0 & -X_p & 0 & 0 & 0 & Y_q & X_pY_q
\end{pmatrix}
$$

Our Matrix

$$f_q(x_q, y_q) = 1 + x_q(y_q - 1) = -x_p + x_q y_q$$

$$\begin{pmatrix}
e & & & & & \\
0 & eX_p & & & & \\
N & NX_p & -X_pY_p & & & \\
0 & 0 & 0 & eY_p & & \\
0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & \\
0 & -X_p & 0 & 0 & 0 & X_qY_q
\end{pmatrix}$$

Our Matrix

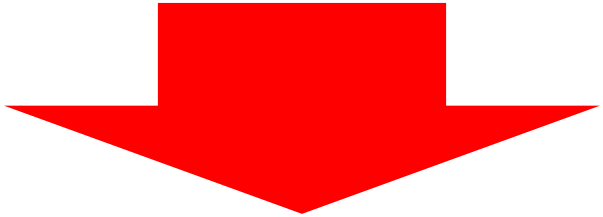
$$\begin{pmatrix}
e & & & & & \\
0 & eX_p & & & & \\
N & NX_p & -X_pY_p & & & \\
0 & 0 & 0 & eY_p & & \\
0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & \\
0 & -X_p & 0 & 0 & 0 & X_qY_q
\end{pmatrix}$$

We can eliminate some polynomials whose diagonals are large.

Overview

$$f_p(x_p, y_p) = 0, \qquad f_q(x_q, y_q) = 0$$

We use either $f_p(x_p, y_p)$ or $f_q(x_q, y_q)$ where the ratio depends on the sizes of p, q.



An algebraic structure of $f_q(x_q, y_q)$ enables us to construct triangular matrices without useless polynomials.

Our Matrix

$$
\begin{pmatrix}
e & & & & & \\
0 & eX_p & & & & \\
N & NX_p & -X_pY_p & & & \\
0 & 0 & 0 & eY_p & & \\
0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & \\
0 & -X_p & 0 & 0 & 0 & X_qY_q
\end{pmatrix}
$$

$m = 1, \lambda = 1/2$

Our Matrix

$$\begin{pmatrix}
e & & & & & \\
0 & eX_p & & & & \\
N & NX_p & -X_pY_p & & & \\
0 & 0 & 0 & eY_p & & \\
0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & \\
0 & -X_p & 0 & 0 & 0 & X_qY_q
\end{pmatrix}$$

Either y_p or y_q appeared in every monomial.

Our Matrix

$$\begin{pmatrix} e & & & & & \\ 0 & eX_p & & & & \\ N & NX_p & -X_pY_p & & & \\ 0 & 0 & 0 & eY_p & & \\ 0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & \\ 0 & -X_p & 0 & 0 & 0 & X_qY_q \end{pmatrix}$$

- x_p appears in monomials that don't have y_q.
- x_q appears in monomials that have y_q.

Our Matrix

$$
\begin{pmatrix}
e^3 & & & & & & & & & & & \\
 & X_p e^3 & & & & & & & & & & \\
 & & X_p^2 e^3 & & & & & & & & & \\
 & & & X_p^3 e^3 & & & & & & & & \\
Ne^2 & NX_p e^2 & & & -X_p Y_p e^2 & & & & & & & \\
 & NX_p e^2 & NX_p^2 e^2 & & & -X_p^2 Y_p e^2 & & & & & & \\
 & & NX_p^2 e^2 & NX_p^3 e^2 & & & -X_p^3 Y_p e^2 & & & & & \\
 & -2X_p e & -2X_p^2 e & & N^{-1} X_p^2 Y_p e & & & X_q^2 Y_q e & & & & \\
 & & -2X_p^2 e & -2X_p^3 e & & N^{-1} X_p^3 Y_p e & -X_q^2 Y_q e & X_q^3 Y_q e & & & & \\
 & -3N^2 X_p & -6N^2 X_p^2 & -3N^2 X_p^3 & 3NX_p^2 Y_p & 3NX_p^3 Y_p & & N^2 X_q^3 Y_q & -X_p^3 Y_p^2 & & & \\
 & -X_p e^2 & & & & & & & & X_q Y_q e^2 & & \\
 & & 3X_p^2 & 3X_p^3 & & -3N^{-1} X_p^3 Y_p & 3X_q^2 Y_q & -3X_q^3 Y_q & & & X_q^3 Y_q^2 &
\end{pmatrix}
$$

$m = 3, \lambda = 1/2$
Triangular for arbitrary large m.

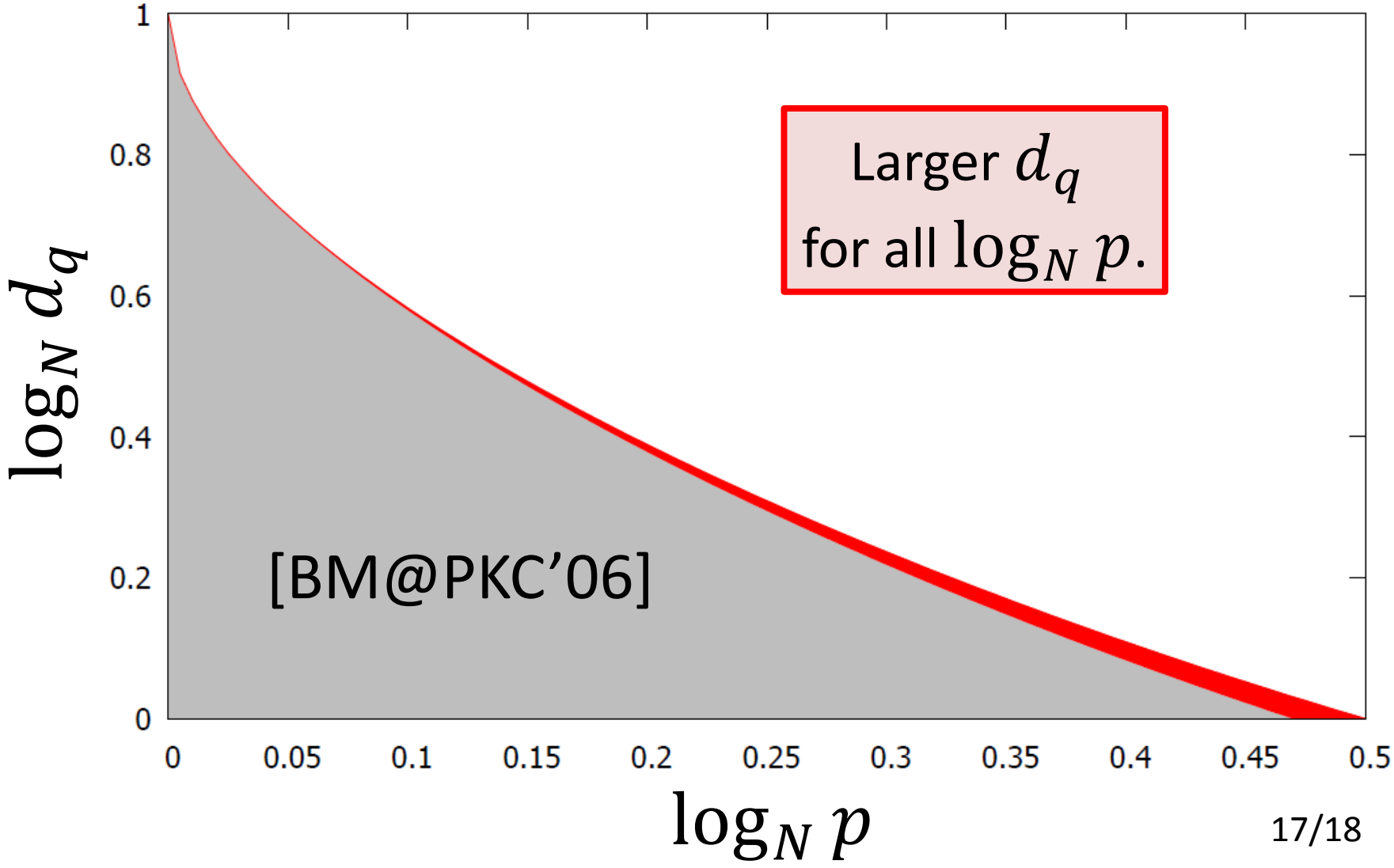
Our Matrix

$$
\begin{pmatrix}
e^3 & & & & & & & & & & & \\
X_p e^3 & & & & & & & & & & & \\
X_p^2 e^3 & & & & & & & & & & & \\
X_p^3 e^3 & & & & & & & & & & & \\
Ne^2 & NX_p e^2 & & & -X_p Y_p e^2 & & & & & & & \\
NX_p e^2 & NX_p^2 e^2 & & & & -X_p^2 Y_p e^2 & & & & & & \\
 & NX_p^2 e^2 & NX_p^3 e^2 & & & & -X_p^3 Y_p e^2 & & & & & \\
N^2 e & 2N^2 X_p e & N^2 X_p^2 e & & -2NX_p Y_p e & -2NX_p^2 Y_p e & & X_p^2 Y_p^2 e & & & & \\
 & N^2 X_p e & 2N^2 X_p^2 e & N^2 X_p^3 e & & -2NX_p^2 Y_p e & -2NX_p^3 Y_p e & & X_p^3 Y_p^2 e & & & \\
 & -3X_p & -6X_p^2 & -3X_p^3 & & 3N^{-1} X_p^2 Y_p & 3N^{-1} X_p^3 Y_p & & -N^{-2} X_p^3 Y_p^2 & X_q^3 Y_q & & \\
 & -X_p e^2 & & & & & & & & & X_q Y_q e^2 & \\
 & -2X_p e & -2X_p^2 e & & & N^{-1} X_p^2 Y_p e & & & & & & X_q^2 Y_q e \\
 & & X_p^2 e & & & & & & & & 2X_q Y_q e & -2X_q^2 Y_q e \\
 & & 3X_p^2 & 3X_p^3 & & & -N^{-1} X_p^3 Y_p & & & -3X_q^3 Y_q & 3X_q^2 Y_q & X_q^3 Y_q^2
\end{pmatrix}
$$

$m = 3, \lambda = 2/3$

Triangular for any λ.

Attack Comparison



Conclusion

- We propose an improved attack on CRT-RSA with small d_q by introducing a new lattice construction technique which is specialized to CRT-RSA.
  - Smaller lattice dimension than previous attacks.
  - Recover larger d_q for any p.
- The technique is applicable to small d_p, d_q attack and variants of CRT-RSA.