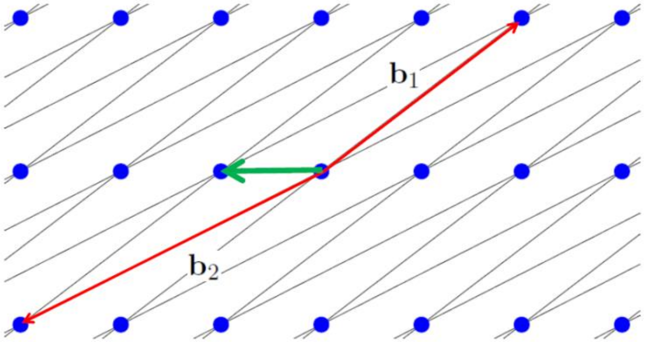


PKC2016@Taipei

How to Generalize RSA Cryptanalyses

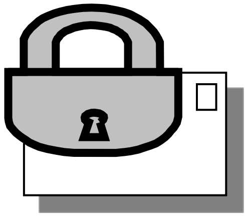
Atsushi Takayasu and Noboru Kunihiro

The University of Tokyo, Japan

AIST, Japan

Background

RSA



Public key: (N, e)

Secret key: (p, q, d)

Key generation: $N = pq$ and

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

✓ One of the most famous cryptosystems

✓ A number of paper study the security.

Known Attacks on RSA

- Small secret exponent attack: [BD00]
  Small secret exponent
  $$d < N^{0.292}$$
  disclose the factorization of N.
- Partial key exposure attacks: [EJMW05], [TK14]
  The most/least significant bits of d disclose the factorization of N.

✓ These attacks are based on Coppersmith's method.

Variants of RSA

	RSA	Takagi RSA	Prime Power RSA
PK	(N, e)	(N, e)	(N, e)
SK	(p, q, d)	(p, q, d)	(p, q, d)
KG	$N = pq$	$N = p^r q$	$N = p^r q$
	$ed = 1 \mod (p-1)(q-1)$	$ed = 1 \mod (p-1)(q-1)$	$ed = 1 \mod p^{r-1}(p-1)(q-1)$

- ✓ The variants enable faster decryption using CRT.
- ✓ When $r = 1$, both variants are the same as RSA.

Known Attacks on the Variants

	RSA	Takagi's RSA	Prime Power RSA
Small Secret Exponent	[BD00]	[IKK08]	[May04], [LZPL15], [Sar15]
Partial Key Exposure	[EJMW05], [TK14]	[HHX+14]	[May04], [LZPL15], [Sar15], [EKU15]

- ✓ When $r = 1$, only [IKK08] achieves the same bound as the best attacks on RSA.

Open Questions

- Are there better attacks on the variants that generalize the best attacks on RSA?
- [IKK08]'s algorithm construction is very technical and hard to follow.

Open Questions

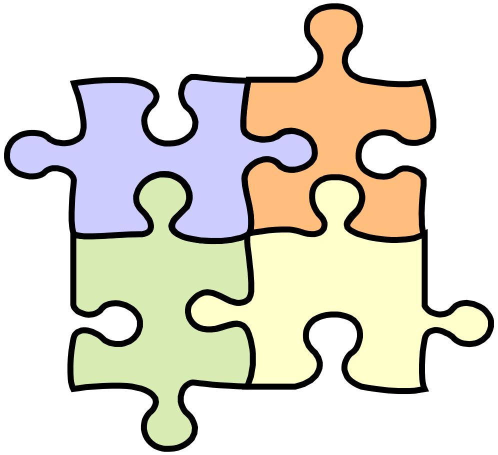
- Are there better attacks on the variants that generalize the best attacks on RSA?
- [IKK08]'s algorithm construction is very technical and hard to follow.

Are there easy-to-understand *generic transformations* that convert the attacks on RSA to Takagi's RSA and the prime power RSA?

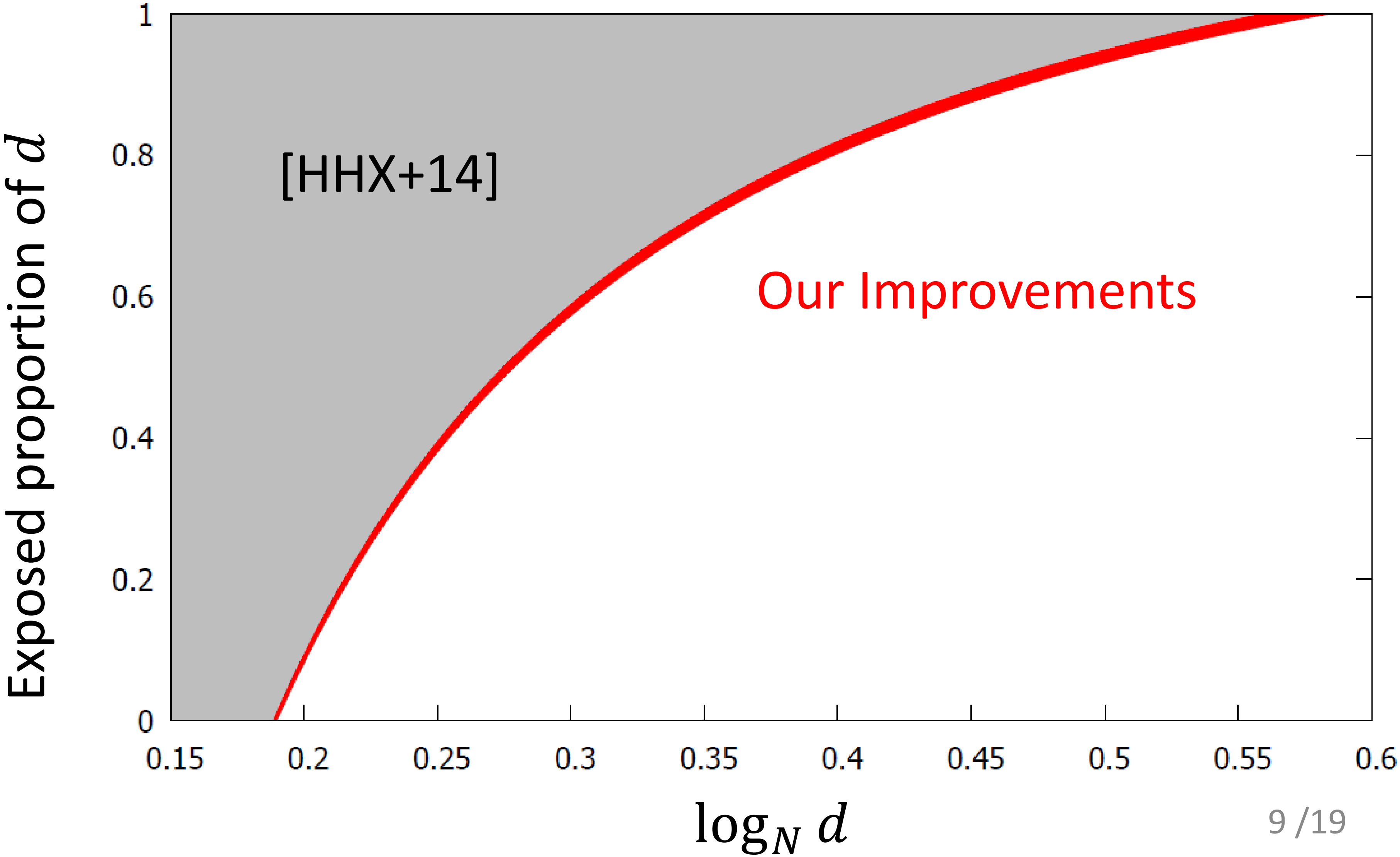
Our Results

We propose transformations for both the Takagi's RSA and the prime power RSA which are very simple and give improved results.

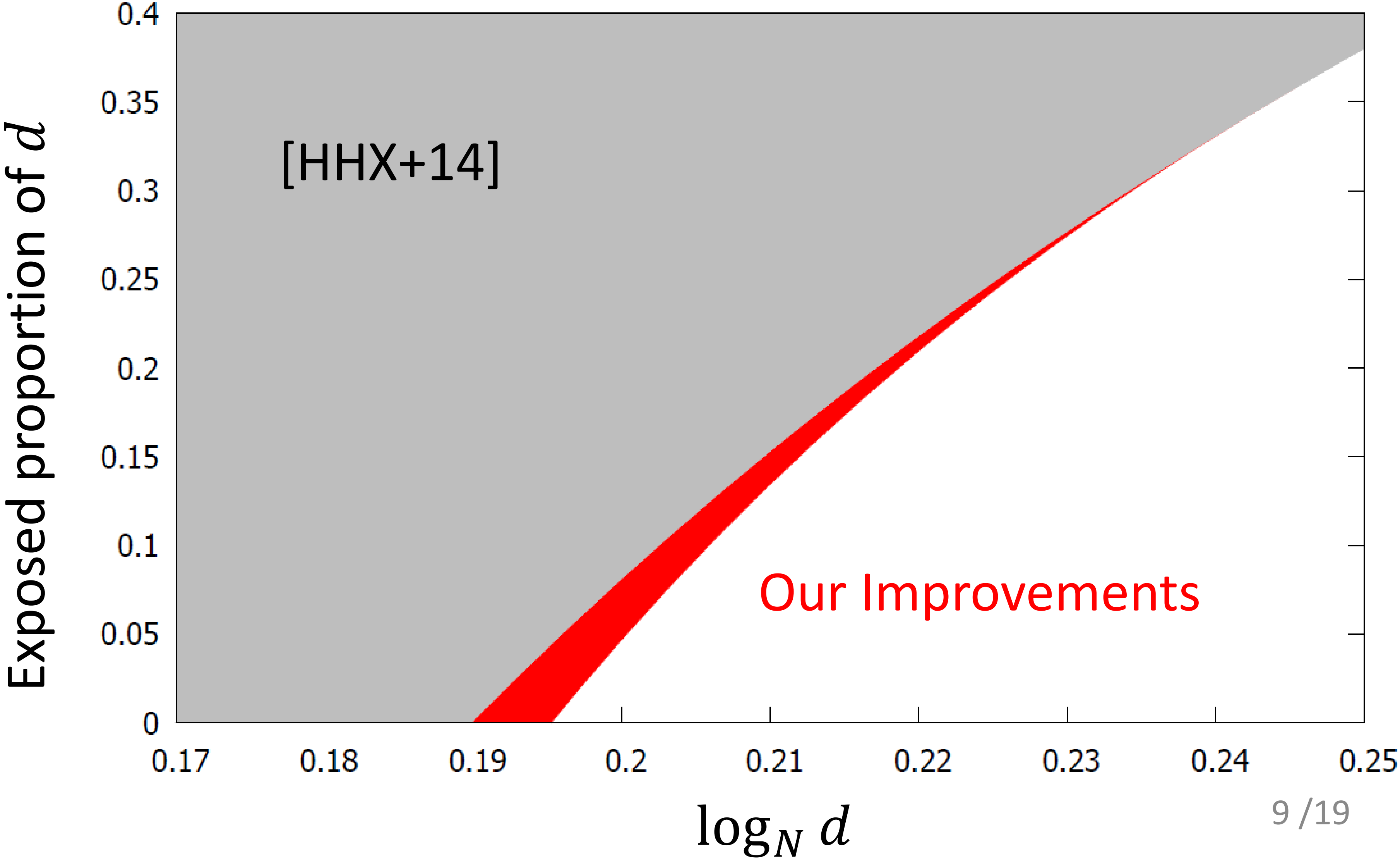
- Simpler analyses of [IKK08], [Sar15]
- Better bounds than [HHX+14], [Sar15], [EKU15]
- Some evidence of optimality



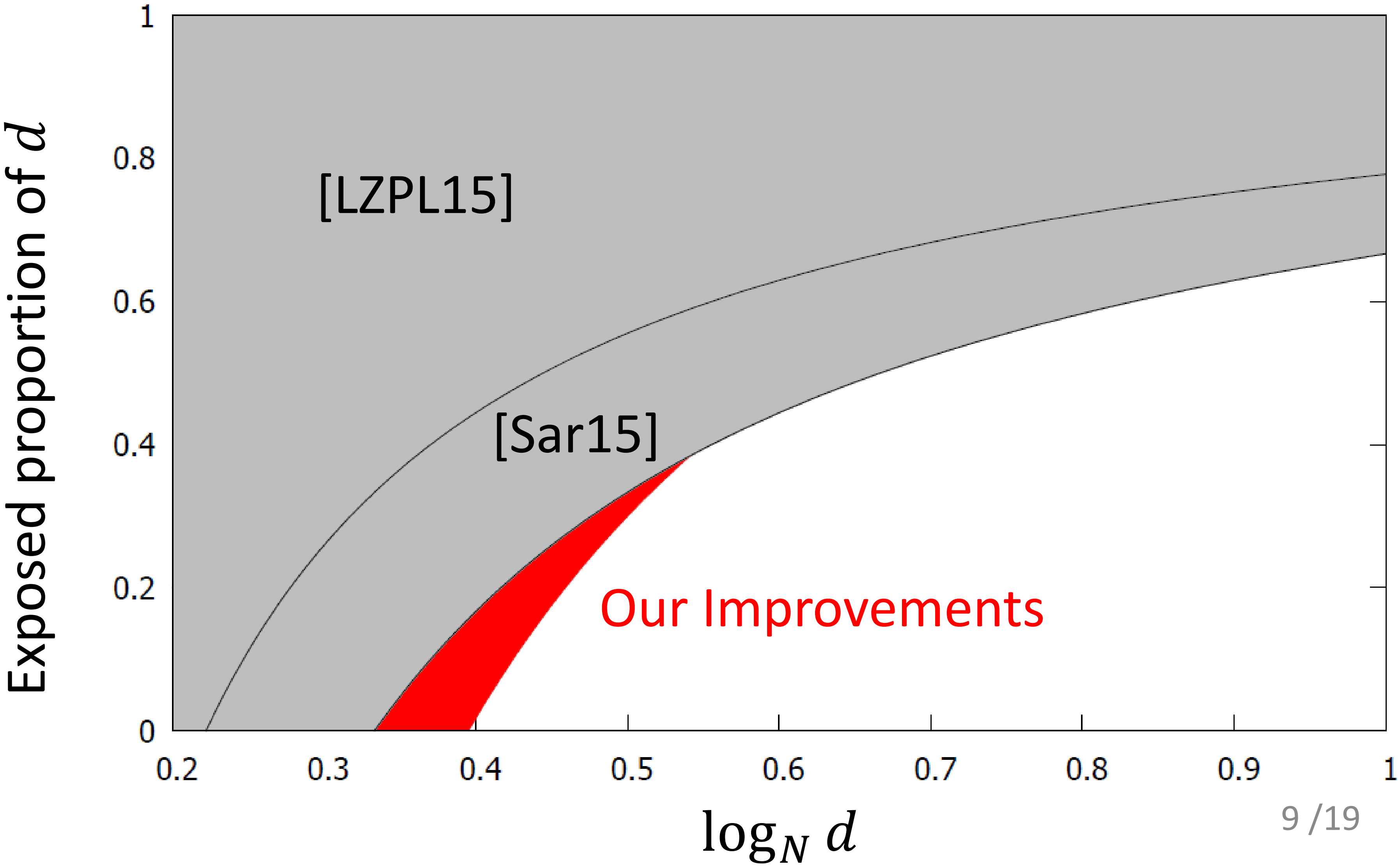
PKE attacks on Takagi's RSA $(r = 2)$



PKE attacks on Takagi's RSA $(r = 2)$



PKE attacks on the prime power RSA $(r = 2)$



Coppersmith's Method

Overview [How97]

To find small roots of a bivariate modular equation

$$h(x, y) = 0 \bmod e$$

where $|\tilde{x}| < X$ and $|\tilde{y}| < \mathrm{Y}$,

Overview [How97]

To find small roots of a bivariate modular equation

$$h(x, y) = 0 \bmod e$$

where $|\tilde{x}| < X$ and $|\tilde{y}| < \mathrm{Y}$,

- Generate $h_1(x, y), \ldots, h_n(x, y)$ that have the roots $(\tilde{x}, \tilde{y})$ modulo e^m.

Overview [How97]

To find small roots of a bivariate modular equation

$$h(x, y) = 0 \bmod e$$

where $|\tilde{x}| < X$ and $|\tilde{y}| < \mathrm{Y}$,

- Generate $h_1(x, y), \dots, h_n(x, y)$ that have the roots $(\tilde{x}, \tilde{y})$ modulo e^m.
- If integer linear combinations of $h_1(x, y), \dots, h_n(x, y)$ become $h_1'(x, y)$ and $h_2'(x, y)$ satisfying

$$\|{h_i}'(xX, yY)\| < e^m,$$

  the original roots can be recovered.

LLL Reduction to Find the Polynomials

- Polynomials $h_1'(x,y)$ and $h_2'(x,y)$ that are the integer linear combinations of $h_1(x,y), \ldots, h_n(x,y)$ and the norms of $\|h_i{}'(xX, yY)\|$ are small.

LLL Reduction to Find the Polynomials

- Polynomials $h'_1(x, y)$ and $h'_2(x, y)$ that are the integer linear combinations of $h_1(x, y), \dots, h_n(x, y)$ and the norms of $\|h_i{}'(xX, yY)\|$ are small.

- LLL algorithm can efficiently find short lattice vectors $\vec{b}_1{}'$ and $\vec{b}_2{}'$ that are the integer linear combinations of $\vec{b}_1$, ..., $\vec{b}_n$ and the Euclidean norms are small.

LLL Reduction to Find the Polynomials

- Polynomials $h_1'(x, y)$ and $h_2'(x, y)$ that are the integer linear combinations of $h_1(x, y), \dots, h_n(x, y)$ and the norms of $\|h_i'(xX, yY)\|$ are small.

⬇

- LLL algorithm can efficiently find short lattice vectors $\vec{b}_1{}'$ and $\vec{b}_2{}'$ that are the integer linear combinations of $\vec{b}_1$, …, $\vec{b}_n$ and the Euclidean norms are small.

✓ Build a lattice whose basis consists of coefficients of $h_1(xX, yY), \dots, h_n(xX, yY)$ and apply the LLL.

SSE Attack on RSA [BD00]

$$N = pq \quad \text{and} \quad ed = 1 \mod (p-1)(q-1)$$
$$f(x,y) = 1 + x(N+1+y) \mod e$$

whose root $(\ell, -(p+q))$ discloses the factorization of N.

- A bivariate equation with three monomials $(1, x, xy)$

SSE Attack on RSA [BD00]

$$N = pq \quad \text{and} \quad ed = 1 \mod (p-1)(q-1)$$
$$f(x,y) = 1 + x(N+1+y) \mod e$$

whose root $(\ell, -(p+q))$ discloses the factorization of N.

Polynomials

$$x^i y^j f^u(x,y) e^{m-u}$$

generate a triangular matrix with diagonals

$$X^{i+u} Y^{j+u} e^{m-u}.$$

✓ The resulting lattice constructions are well-analyzed.

SSE Attack on RSA [BD00]

$$N = pq \quad \text{and} \quad ed = 1 \mod (p-1)(q-1)$$
$$f(x,y) = 1 + x(N+1+y) \mod e$$

whose root $(\ell, -(p+q))$ discloses the factorization of N.

Polynomials

$$x^i y^j f^u(x,y) e^{m-u}$$

generate a triangular matrix with diagonals

$$X^{i+u} Y^{j+u} e^{m-u}.$$

✓ The resulting lattice constructions are well-analyzed.

How to Generalize the Attacks

SSE Attack on Takagi's RSA

$$N = p^r q \quad \text{and} \quad ed = 1 \mod (p-1)(q-1)$$
$$f(x, y_1, y_2) = 1 + x(y_1 - 1)(y_2 - 1) \mod e$$

whose root (ℓ, p, q) discloses the factorization of N.

- A trivariate equation with five monomials $(1, x, xy_1, xy_2, xy_1y_2)$
- Nontrivial algebraic relation $y_1^r y_2 = N$

SSE Attack on Takagi's RSA

$$N = p^r q \quad \text{and} \quad ed = 1 \mod (p-1)(q-1)$$
$$f(x, y_1, y_2) = 1 + x(y_1 - 1)(y_2 - 1) \mod e$$

whose root (ℓ, p, q) discloses the factorization of N.

Polynomials

$$\{1, y_2, y_1 y_2, \dots, y_1^{r-1} y_2\} \cdot x^i y_1^j f^u(x, y_1, y_2) e^{m-u}$$

generate a triangular matrix with (sizes of) diagonals

$$\{Y^0, Y^1, \dots, Y^r\} \cdot X^{i+u} Y^{j+u} e^{m-u}.$$

SSE Attack on Takagi's RSA

$$N = p^r q \quad \text{and} \quad ed = 1 \mod (p-1)(q-1)$$
$$f(x, y_1, y_2) = 1 + x(y_1 - 1)(y_2 - 1) \mod e$$

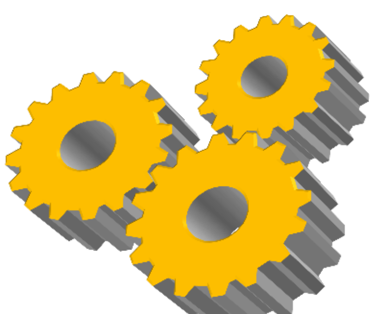
whose root (ℓ, p, q) discloses the factorization of N.

Polynomials

$$\{1, y_2, y_1 y_2, \dots, y_1^{r-1} y_2\} \cdot x^i y_1^j f^u(x, y_1, y_2) e^{m-u}$$

generate a triangular matrix with (sizes of) diagonals

$$\{Y^0, Y^1, \dots, Y^r\} \cdot X^{i+u} Y^{j+u} e^{m-u}.$$



SSE Attack on the prime power RSA

$$N = p^r q \quad \text{and} \quad ed = 1 \mod (p-1)(q-1)$$
$$f(x, y_1, y_2) = 1 + xy_1^{r-1}(y_1 - 1)(y_2 - 1) \mod e$$
whose roots (ℓ, p, q) offer the factorization of N.

- A trivariate equation with five monomials $(1, x, xy_1^{r-1}, xy_1^r, xy_1^{r-1}y_2)$
- Nontrivial algebraic relation $y_1^r y_2 = N$

SSE Attack on the prime power RSA

$$N = p^r q \quad \text{and} \quad ed = 1 \mod (p-1)(q-1)$$

$$f(x, y_1, y_2) = 1 + x y_1^{r-1}(y_1 - 1)(y_2 - 1) \mod e$$

whose roots (ℓ, p, q) offer the factorization of N.

Polynomials

$$\{y_2^a, y_1 y_2^a, \ldots, y_1^{r-1} y_2^a, y_1^{r-1} y_2^{a+1}\}$$

$$\cdot\, x^i y_1^j f^u(x, y_1, y_2) e^{m-u}$$

generate a triangular matrix with (sizes of) diagonals

$$\{Y^a, Y^{a+1}, \ldots, Y^{a+r}\} \cdot X^{i+u} Y^{j+u} e^{m-u}.$$

Our Transformations

SSE on RSA

PKE on RSA

$\{1, y_2, y_1 y_2, \ldots, y_1^{r-1} y_2\}$

SSE on Takagi RSA

PKE on Takagi RSA

Our Transformations

SSE on RSA

PKE on RSA

$$\{y_2^a, y_1 y_2^a, \ldots, y_1^{r-1} y_2^a, y_1^{r-1} y_2^{a+1}\}$$

SSE on prime power RSA

PKE on prime power RSA

Conclusion

- We propose *generic transformations* that convert lattices on RSA to those on the Takagi RSA and the prime power RSA.
  As applications, we propose small secret exponent attacks and partial key exposure attacks on the variants.

✓ Further applications of our transformations?

✓ Better attacks can be obtained from other frameworks?