RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: CRYP-R01

Finding Shortest Lattice Vectors in the Presence of Gaps

Wei Wei [1], Mingjie Liu[2], Xiaoyun Wang[3]

[1] Institute of Information Engineering, Chinese Academy of Sciences, China/ Post-doc Researcher

[2] Research Institute of Telemetry, [3]Tsinghua University, China

April 23, 2015

#RSAC

Outline

- Motivation
- Revisit SVP Algorithms on Lattices with Gaps
- Search SVP for Some Lattice-based Cryptosystems
- Summary

Motivation

Shortest Vector Problem

- SVP: NP-Hard
  - Given a basis of a lattice, find a nonzero shortest lattice vector.
- uSVP$_\gamma$: unique-Shortest Vector Problem
  - $\lambda_2(L) > \gamma\lambda_1(L)$, find a nonzero shortest lattice vector.
- SVP algorithms
  - Deterministic: enumeration, Voronoi cell computation based…
  - Probabilistic: heuristic & **provable sieve**…

Previous Work

- Probabilistic Sieve algorithms:
  - **Heuristic**:

Algorithm	Time	Space
Nguyen, Vidick (2008)	$2^{0.415n}$	$2^{0.2075n}$
Wang, et al. (2011)	$2^{0.3836n}$	$2^{0.2557n}$
Zhang, et. al. (2013)	$2^{0.3778n}$	$2^{0.2833n}$
Becker, et. al. (2013)	$2^{0.3774n}$	$2^{0.2925n}$

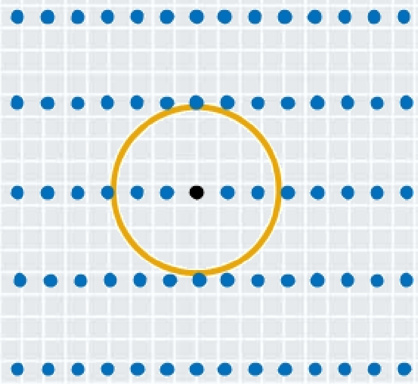
Previous Work

- Probabilistic Sieve algorithms:
  - **Provable**:

Algorithm	Time	Space	Reference
AKS	$2^{O(n)}$	$2^{O(n)}$	[Ajtai,et al. 2001]
Regev	2^{16n}	2^{8n}	[Regev 2004]
NV	$2^{5.9n}$	2^{3n}	[Nguyen, Vidick 2008]
ListSieve	$2^{3.199n}$	$2^{1.325n}$	[Micciancio, Voulgaris 2009]
ListSieve-Birthday	$2^{2.465n}$	$2^{1.233n}$	[Pujol, Stehlé 2009]

Motivation

- What about lattices with **gaps**?
  - Successive minima $\lambda_2(L) > \gamma\lambda_1(L)$
  - Sparse distribution
  - Complexity decreases obviously as the increase of gap
  - Common in cryptographic instances



RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

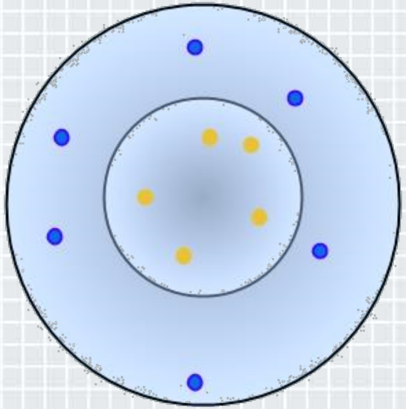
SVP Algorithms on Lattices with Gaps

List-Sieve [MV09]

- Creat a set of short vectors by subtractions.
- All previous vectors are used to reduce a new one.
- Random perturbation technique.
- Several lattice vectors might correspond to one perturbed vector.
- A collision happens with a high probability when there are enough sieved vectors.

ListSieve-Birthday[PS09]

- Apply List-Sieve, sample lattice points that fall inside of the corona which consist of the first list.
- Sample **small** and **independent** points by reducing random points with respect to the first list.
- A collision occurs with high probability.

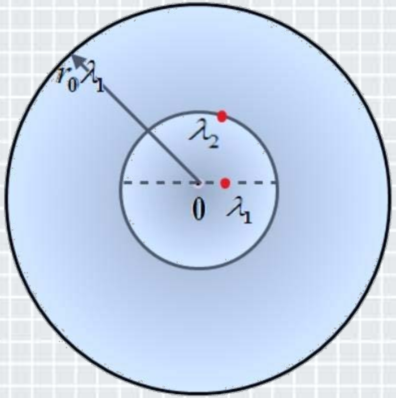


Revisit Sieve Algorithms on Lattices with Gaps

- Two cases
  - λ_2-gap: $\lambda_2(L) > \alpha\lambda_1(L)$
  - λ_{i+1}-gap: $\lambda_{i+1}(L) > \alpha\lambda_1(L)$
- Concretely
  - **Packing density** of lattices with gaps
  - ListSieve-Birthday

Packing density of lattices with λ_2-gap

What is the maximum number of lattice points inside a sphere with radius $r_0\lambda_1$?



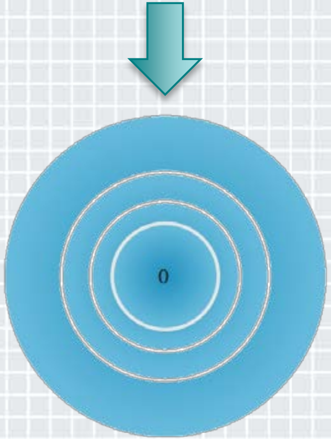
- Our result: If $\lambda_2(L) > \alpha\lambda_1(L)$, then

$$|\mathcal{B}_n(\mathbf{0}, r_0\lambda_1) \cap L| \leq 2^{c_b n + o(n)},$$

where $c_b = \log_2 r_0 - \log_2 \alpha + 0.401$ and $1 \leq \alpha \leq r_0$.

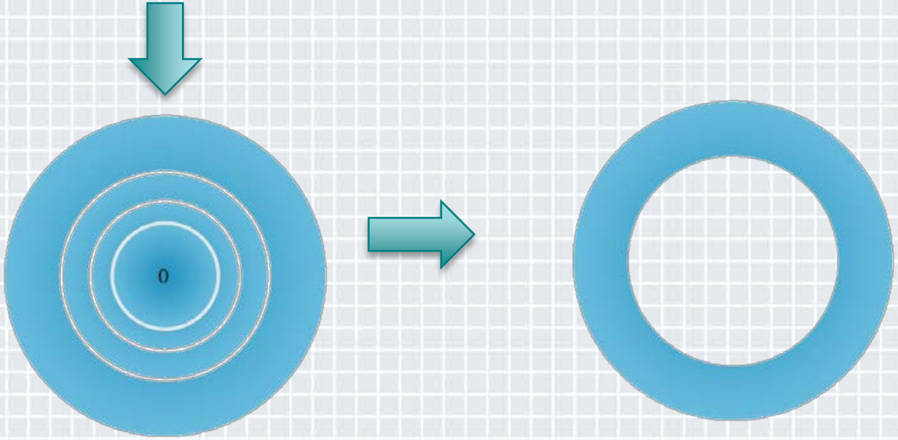
Count the Number of Points

Partition into coronas

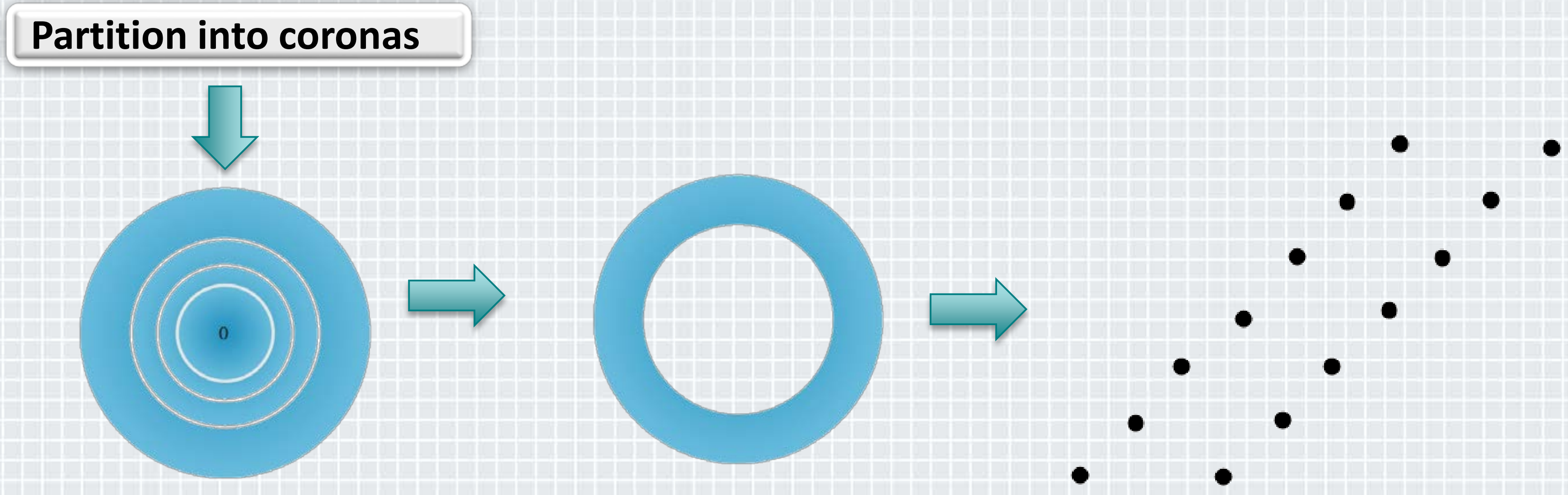


Count the Number of Points

Partition into coronas

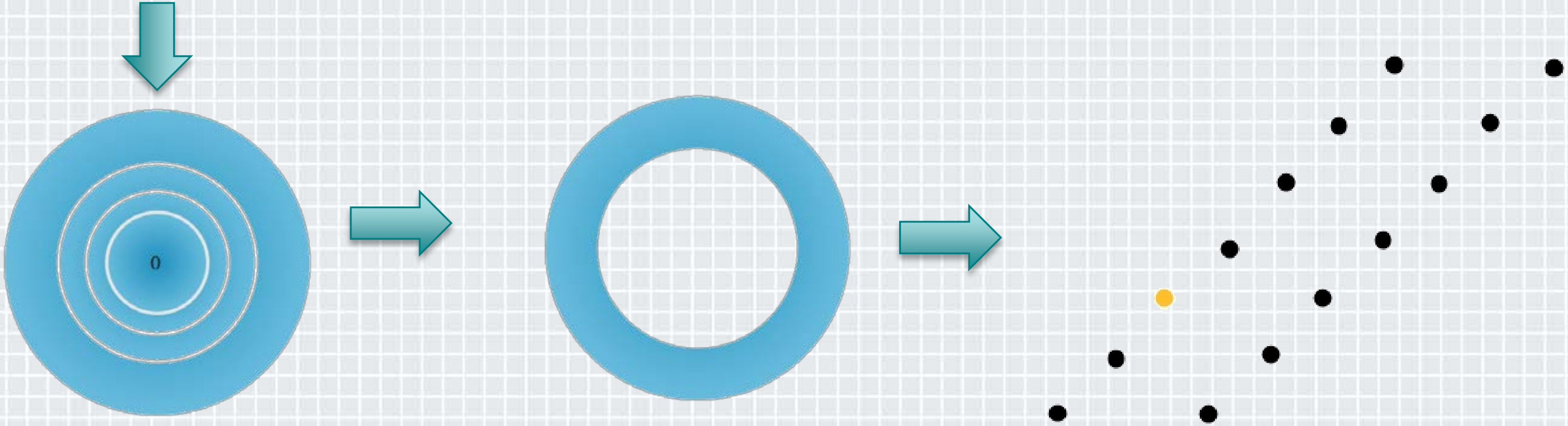


Count the Number of Points

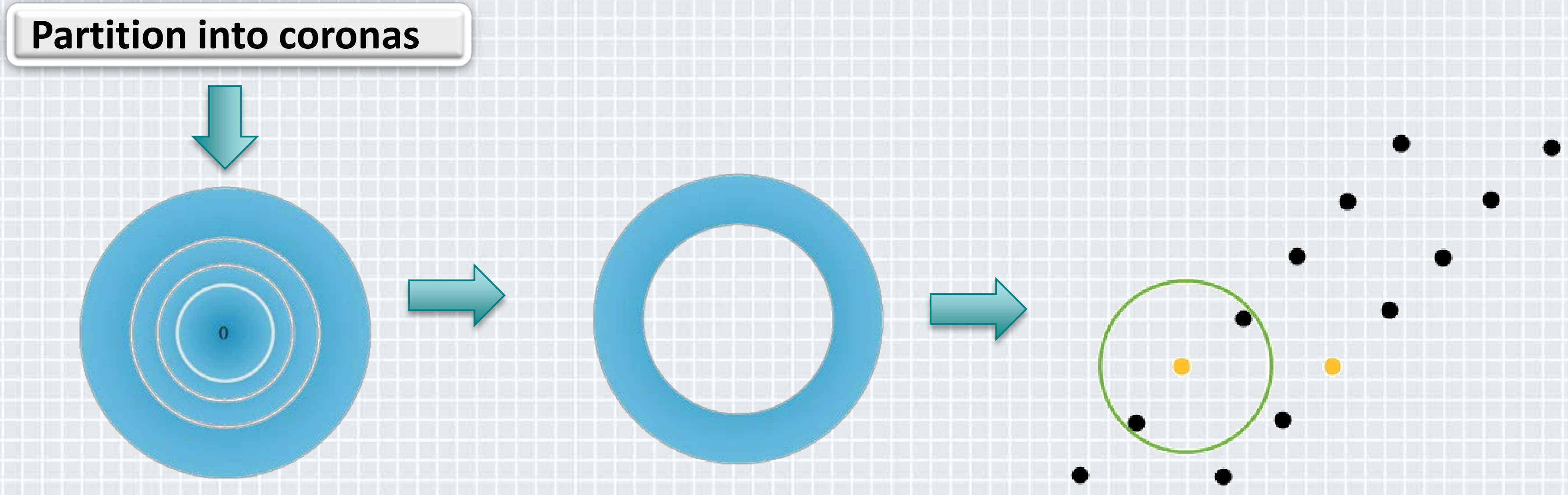


Count the Number of Points

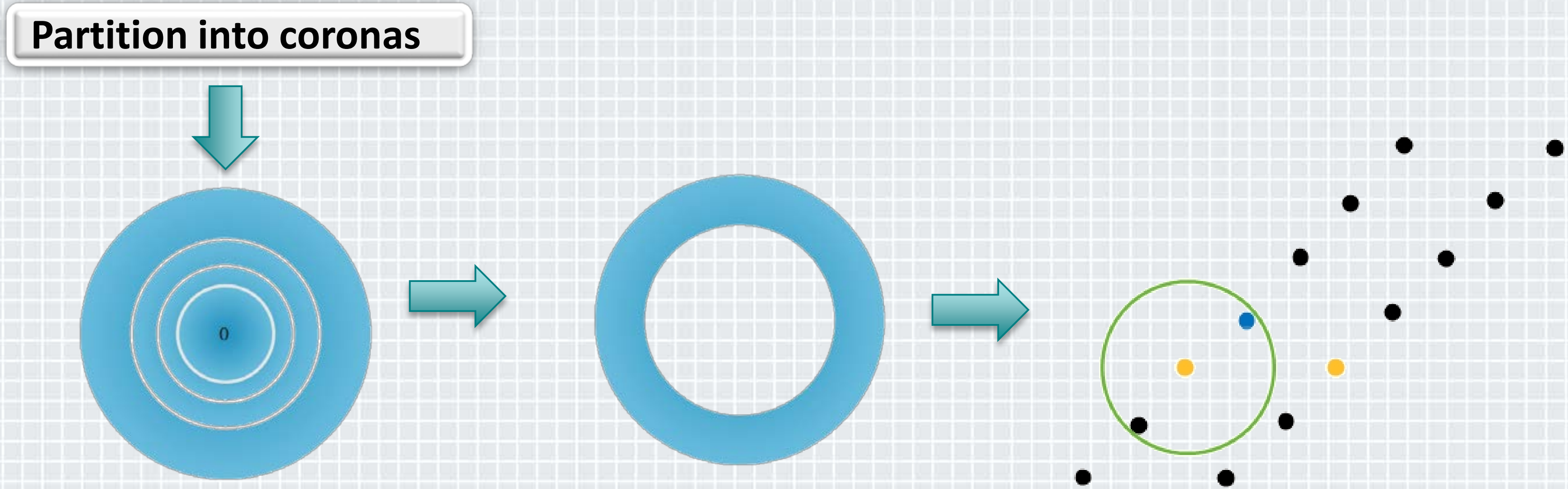
Partition into coronas



Count the Number of Points

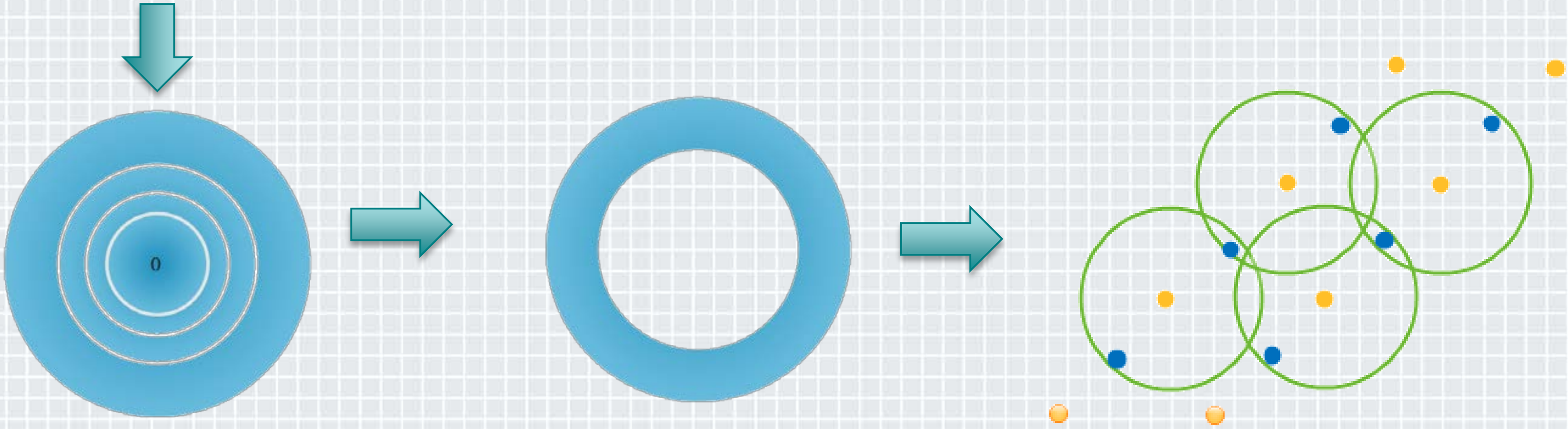


Count the Number of Points



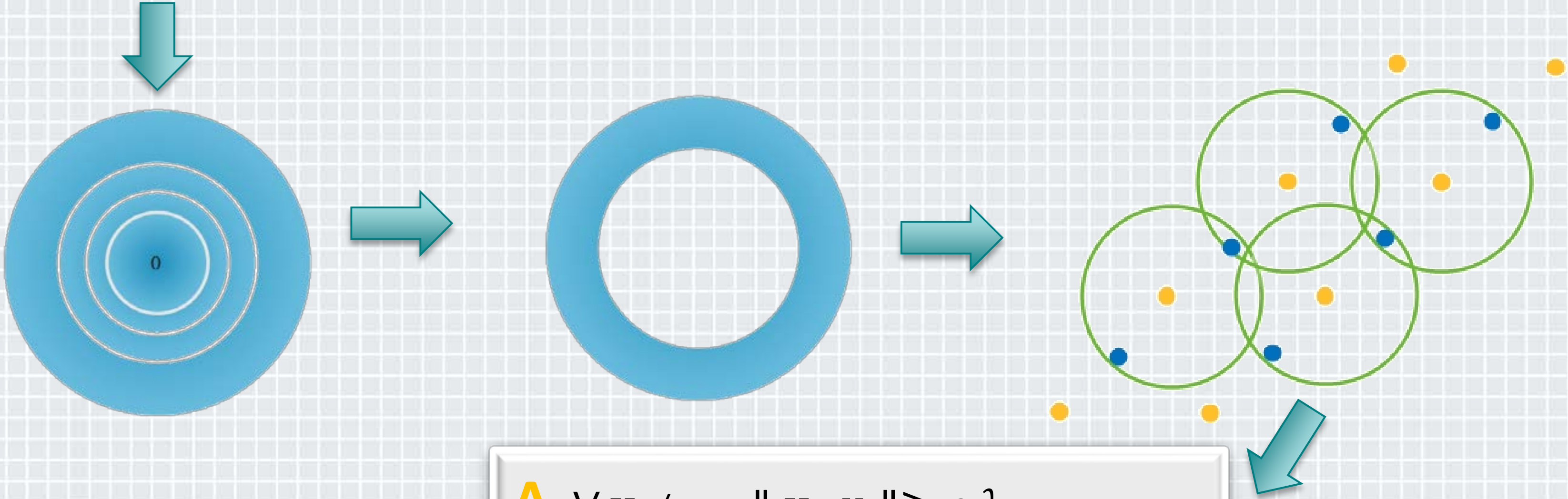
Count the Number of Points

Partition into coronas



Count the Number of Points

Partition into coronas

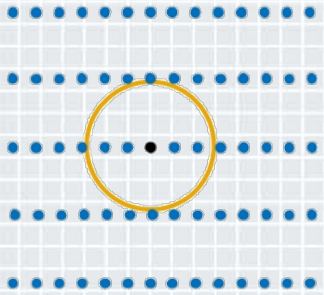


$\mathbf{A}$: $\forall\ \mathbf{v} \neq \mathrm{u},\ \| \mathbf{v}-\mathbf{u} \| \geq \alpha\lambda_1$

$\mathbf{B} = \{\mathbf{w}\!:\ \exists\ \mathbf{t} \in \mathbf{A},\ \text{s.t.}\ \| \mathbf{w}-\mathbf{t} \| < \alpha\lambda_1\}$

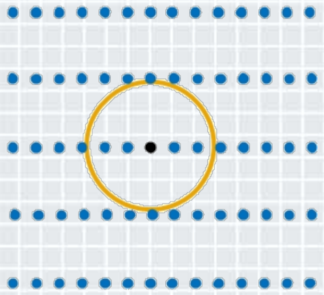
Estimate |A|, |B|

- $|\mathbf{B}| \le (1 + 2\lfloor \alpha \rfloor)|\mathbf{A}|$

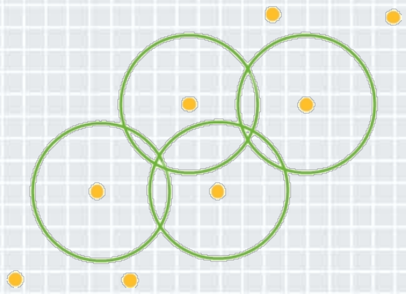


Estimate |A|, |B|

- $|\mathbf{B}| \leq (1 + 2\lfloor\alpha\rfloor)|\mathbf{A}|$

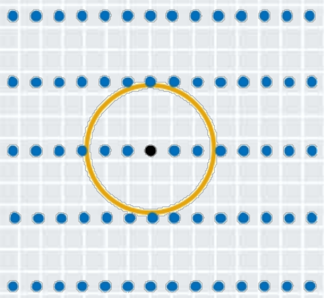


- $|\mathbf{A}| \leq 2^{(\log_2 r_0 - \log_2 \alpha + 0.401)n + o(n)}$

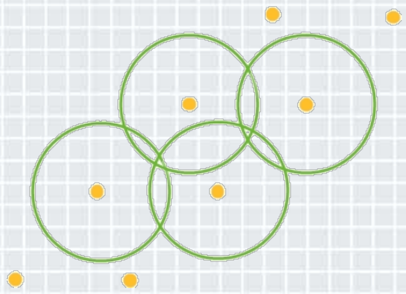


Estimate |A|, |B|

- $|\mathbf{B}| \leq (1 + 2\lfloor\alpha\rfloor)|\mathbf{A}|$



- $|\mathbf{A}| \leq 2^{(\log_2 r_0 - \log_2 \alpha + 0.401)n + o(n)}$



- Finally, $|\mathcal{B}_n(\mathbf{0}, r_0\lambda_1) \cap L| \leq \mathrm{poly}(n) \cdot (|\mathbf{A}| + |\mathbf{B}|) \leq 2^{c_b n + o(n)}$

Complexity Analysis of ListSieve-Birthday

- Time: $2^{c_{time}n+o(n)}$, Space: $2^{c_{space}n+o(n)}$
- Minimize the time complexity,

$$c_{time} = 0.802 + \log_2\left(\frac{1}{\sqrt{1-\frac{1}{4\xi^2}}} + \frac{2\xi}{\alpha \cdot 2^{0.401}\left(1-\frac{1}{4\xi^2}\right)}\right).$$

- When λ_2-gap >1.78, $c_{time} < 2$, $c_{space} < 1$ by selecting $\xi = 1.0015$.

c_{time}s corresponding to different λ_2-gap

α	ξ	r_0	c_{time} gap
1.78	1.0020	4.0409	1.9969
5	1.1768	8.3301	1.4246
8	1.2992	12.3483	1.2585
12	1.4308	17.7075	1.1502
28	1.7952	39.0991	0.9992
100	2.6293	134.8910	0.8859
500	4.4019	664.7420	0.8306

Sieve for SVP with λ_{i+1}-gap

- **λ_{i+1}-gap**

  $\lambda_{i+1}(L) > \alpha\lambda_1(L), 1 \le i \le n-1$

- **NTRU lattice**

  λ_{N+1}-gap ([HPS98], heuristic)

- **Packing density**

$$|\boldsymbol{\mathcal{B}}_n(\mathbf{0}, r_0\lambda_1) \cap L| \le 2^{(\log_2 r_0 - \log_2 \alpha + 0.401)n + (\log_2 \alpha + 0.401)i + o(n)}.$$

Sieve for SVP with λ_{i+1}-gap

- $c_{time} = 0.802 + \log_2\left(\frac{1}{\sqrt{1-\frac{1}{4\xi^2}}} + \frac{2\xi}{(\alpha\cdot 2^{0.401})^{(1-\frac{i}{n})}(1-\frac{1}{4\xi^2})}\right).$

i \ α	1.78	5	8	12	28	100	500
$\frac{n}{16}$	1.9225	1.4282	1.2767	1.1744	1.0244	0.9035	0.8393
$\frac{n}{8}$	1.9574	1.4757	1.3231	1.2180	1.0597	0.9261	0.8508
$\frac{n}{4}$	2.0297	1.5805	1.4287	1.3200	1.1473	0.9875	0.8857
$\frac{n}{2}$	2.1848	1.8337	1.7000	1.5968	1.4145	1.2116	1.0455
$\frac{3n}{4}$	2.3541	2.1513	2.0658	1.9956	1.8587	1.6777	1.4876

Sieve for SVP with λ_{i+1}-gap

- $c_{time} = 0.802 + \log_2\left(\frac{1}{\sqrt{1-\frac{1}{4\xi^2}}} + \frac{2\xi}{(\alpha\cdot 2^{0.401})^{(1-\frac{i}{n})}(1-\frac{1}{4\xi^2})}\right).$

i \ α	1.78	5	8	12	28	100	500
$\frac{n}{16}$	1.9225	1.4282	1.2767	1.1744	1.0244	0.9035	0.8393
$\frac{n}{8}$	1.9574	1.4757	1.3231	1.2180	1.0597	0.9261	0.8508
$\frac{n}{4}$	2.0297	1.5805	1.4287	1.3200	1.1473	0.9875	0.8857
$\frac{n}{2}$	2.1848	1.8337	1.7000	1.5968	1.4145	1.2116	1.0455
$\frac{3n}{4}$	2.3541	2.1513	2.0658	1.9956	1.8587	1.6777	1.4876

Complexity depends on the **value** and **location** of gap!

RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

Search SVP for Some Lattice-based Systems

Search SVP for Some Lattice-based Systems

- LWE (Learning with Errors)-based cryptosystem
  - A BDD instance in the q-ary lattice
    $$\Lambda_q(\mathbf{A}^T) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{y} = \mathbf{As} \bmod q \text{ for } s \in \mathbb{Z}_q^n\}.$$
  - [LW11] gave its λ_2-gap of the embedding lattice.
  - Our result: For the parameter $n = 128$ in the scheme[Gentry et. al.'08],
    - **λ_2-gap $\approx$ 1288**.
    - Time: $2^{0.8172m+o(m)}$.
    - Space: $2^{0.4086m+o(m)}$.
    - Approximately to $2^{0.802m+o(m)}$ ($2^{0.401m+o(m)}$).

Search SVP for Some Lattice-based Systems

- GGH encryption cryptosystem [Goldreich, Goldwasser, Halevi'97]
  - A BDD-based cryptosystem
  - five challenges: n=200, 250, 300, 350, 400.
  - [Nguyen’99] Four of them are solved and it is indicated the excepted **λ_2-gap> 9.4**.
  - Our result: The time complexity of ListSieve-Birthday is $2^{1.212n+o(n)}$.

Search SVP for Some Lattice-based Systems

- Worst-case/average-case equivalent cryptosystems
  - uSVP_{n^c} based: [Ajtai, Dwork'97, Regev'04].
  - GapSVP_{n^c} based: [Regev'09, Peikert'09].

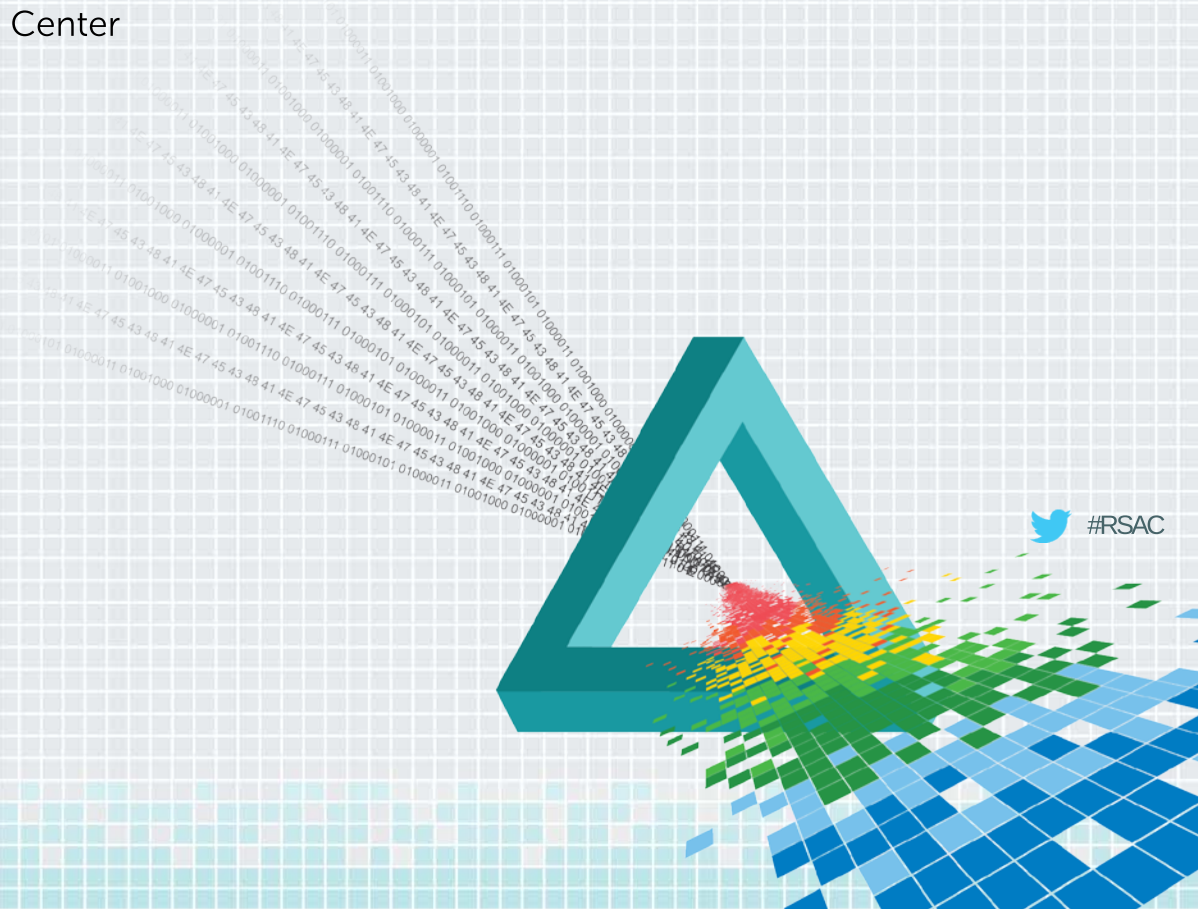
    Then can be equivalently based on $\mathrm{uSVP}_{\tilde{O}(n^c)}$ since the reduction from uSVP_{γ} to GapSVP_{γ}.
  - Our result: Time complexity is approximately to $2^{0.802n+o(n)}$.

Search SVP for some lattice-based systems

- NTRU encryption cryptosystem [Hoffstein, Pipher, Silverman'98]
  - Adopted to standard of IEEE Std 1363.1 in 2008.
  - [HPS98] Heuristically, the NTRU lattice (dimension=2N) has a λ_{N+1}-gap approximately $\sqrt{\frac{Nq}{4\pi e(d_f \cdot d_g)^{1/2}}}\lambda_1$.
  - For $N = 503, q = 256, d_f = 216, d_g = 72,$ the time to solve this SVP of NTRU lattice is $2^{1.8054n+o(n)}$.

RSAConference2015

San Francisco | April 20-24 | Moscone Center



#RSAC

Summary

Summary

- Study SVP on a lattices possessing gaps
  - New upper bounds for the packing density of lattices with λ_i-gap.
  - Renew the complexity of the ListSieve-Birthday
- Discussions on SVP search for some lattice-based cryptosystems
  - LWE-based, GGH, NTRU…
  - Cryptographic lattices should avoid large gaps.

Thank you for your attention!

RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: CRYP-R01

A Simple and Improved Algorithm for Integer Factorization with Implicit Hints

***Koji Nuida[1], Naoto Itakura[2], Kaoru Kurosawa[2]**

[1] AIST, Japan / JST PRESTO Researcher

[2] Ibaraki University, Japan

April 23, 2015

#RSAC

Contents

- Introduction: Integer factoring with implicit hints for LSBs of factors
- Our results
  - Algorithm: Better bound, simpler proof
  - (Potential) application to “(batch) FHE over integers” etc.
- Details and computer experiments

RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

Introduction

Background: Cryptography and Factoring

- Computational hardness of integer factoring is:
  - Necessary (and sometimes sufficient) for security of many cryptosystems
    - Including the RSA cryptosystem
  - Therefore, important to analyze

Background: Factoring with Hints

- Factoring with **explicit** hints
  - E.g., [Coppersmith 1996], where some bits of the factors are known
  - Related to: Side-channel attacks
- Factoring with ***implicit*** hints (**this work**)
  - E.g., [May-Ritzenhofen 2009], where only some ***relations*** of bits of the factors are known
  - Related to: Attacks on implementation with weak randomness

Factoring with Implicit Hints

- Simplest case ([MR09], [Kurosawa-Ueda 2013]):
  For two integers $N_1 = p_1 q_1, N_2 = p_2 q_2$, assume

  (t LSBs of p_1) = (t LSBs of p_2)

  - Or equivalently, $\boldsymbol{p_1 \equiv p_2 \ (mod\ 2^t)}$

- Generalizations (*not considered in this work*):
  - More integers ([MR09], [Sarkar-Maitra 2011], …)
  - MSBs, or combination of LSBs and MSBs ([SM11], …)

Previous Results

- Assume $N_1 = p_1 q_1, N_2 = p_2 q_2$ and $\boldsymbol{p_1 \equiv p_2 \ (mod\ 2^t)}$
- Also assume $\boldsymbol{q_1, q_2 < 2^\alpha}$ (i.e., q_1, q_2 are α-bit primes)
- Polynomial-time factoring of N_1, N_2, if
  - [MR09] $t \geq 2\alpha + 3$
  - [KU13] $t \geq 2\alpha + 1$

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Our Result: Summary

#RSAC

Our Result

- Assume $N_1 = p_1 q_1, N_2 = p_2 q_2$ and $\boldsymbol{p_1 \equiv p_2 \ (mod\ 2^t)}$
- Also assume $\boldsymbol{q_1, q_2 < 2^\alpha}$ (i.e., q_1, q_2 are α-bit primes)
- Polynomial-time factoring of N_1, N_2, if
  - [MR09] $t \geq 2\alpha + 3$
  - [KU13] $t \geq 2\alpha + 1$
  - **Our result**: $\boldsymbol{t = 2\alpha - O(\log \kappa)}$, where κ is a parameter (e.g., security parameter of a factoring-based cryptosystem)

Non-constant improvement!

Advantage: Simplicity and Generality

- Our result (as well as [KU13]) extends to $p_1 \equiv p_2 \ (mod\ \boldsymbol{T})$ and $q_1, q_2 \leq \boldsymbol{Q}$ for integers T, Q
  - Originally $T = 2^t,\ Q = \ 2^\alpha$
- We do ***NOT*** assume that p_1, p_2, q_1, q_2 are primes
  - Only assume that N_1, N_2, T are mutually coprime (almost automatic)
- Very simple, easy-to-follow proof
  - No lattice inequalities (Minkowski bound, Hadamard's inequality, …)

Related Work

- Factors p_1, p_2, q_1, q_2 in [SM11] (and some others)
  - Prime
  - Balanced (i.e., $|p_i|_2 \approx |q_i|_2$)
    - In fact, their result requires $|p_i|_2$ to be bounded above
- Factors p_1, p_2, q_1, q_2 in our result
  - **Not necessarily prime** — **Good**
  - **Unbalanced** (i.e., $|p_i|_2 \gg |q_i|_2$) — **Sometimes good (next slide)**
    - $|p_i|_2$ is bounded below only by the condition $t = 2\alpha - O(\log \kappa)$

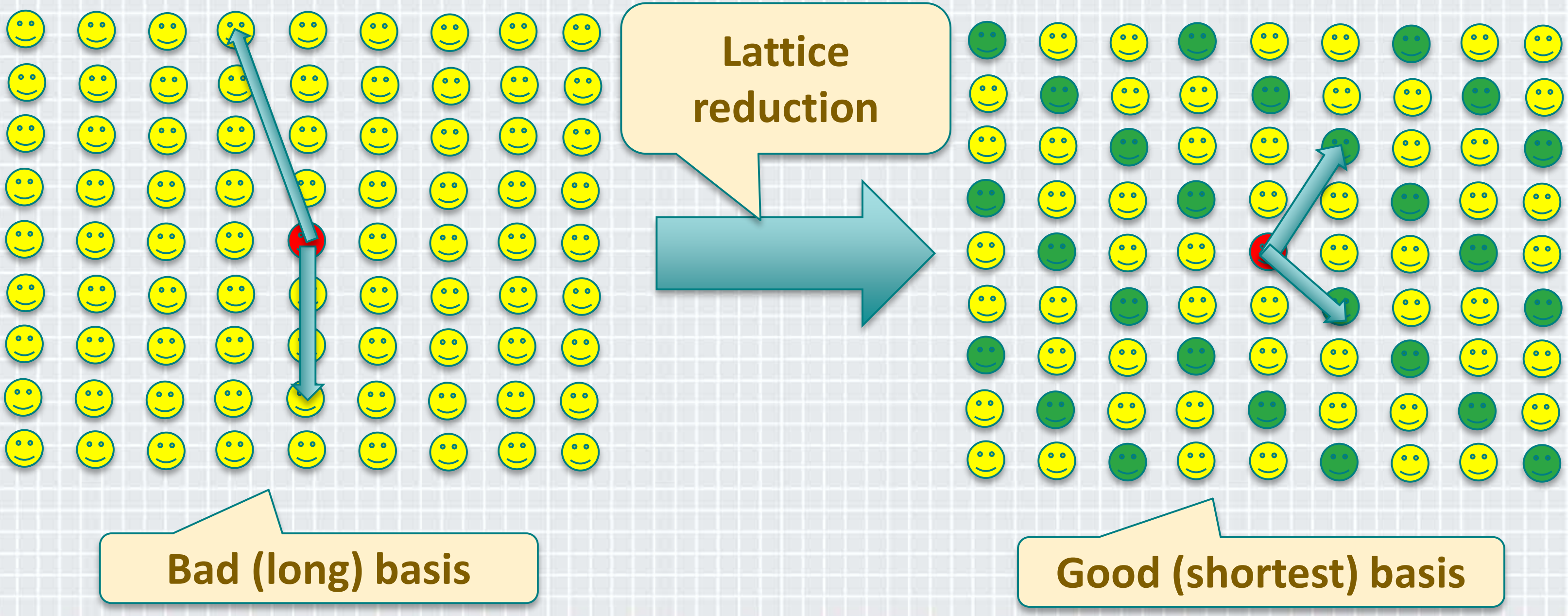
(Potential) Applications

- Variants of (batch) "fully homomorphic encryption over integers" with error-free approximate GCD assumptions [Cheon et al. 2013], [N.-Kurosawa, EUROCRYPT 2015]
  - Ciphertexts are integers modulo $N = qp_1p_2 \cdots p_k$, where $|q|_2 \gg |p_i|_2$
  - Apply our result to factors p_i and $\boldsymbol{N/p_i}$ (**unbalanced**, **non-prime**)
- Okamoto-Uchiyama cryptosystem, Takagi's variant of RSA
  - $N = \boldsymbol{p^r}q, r \geq 2$ (**unbalanced**, **non-prime**)

Our Result: Details

(Integer) Lattice and Basis Reduction

- Lattice in 2-dim. plane



Lattice for Our Problem

- $L = \{(x_1, x_2) \in \mathbb{Z}^2 : N_2 x_1 - N_1 x_2 \equiv 0 \ (mod\ T)\}$

  (recall $N_1 = p_1 q_1, N_2 = p_2 q_2, p_1 \equiv p_2 \ (mod\ T)$)

  - Same as previous work
  - L and initial basis $(1, N_2/N_1\ mod\ T), (0, T)$ are publicly known
  - Involves secret vector $\vec{q} = (q_1, q_2)$

Find this!

Previous Results

- Outline of [KU13]:
  - Find the shortest vector $\vec{v}$ in 2-dim. lattice L by Gaussian reduction
  - If **(*) the second shortest basis vector of L is longer than $\vec{q}$**, then $\vec{\boldsymbol{q}} \propto \vec{v}$, in particular $\vec{\boldsymbol{q}} = (\boldsymbol{q_1}, \boldsymbol{q_2}) = \pm\vec{\boldsymbol{v}}$ (since q_1, q_2 are coprime)
  - (*) is guaranteed when $t \geq 2\alpha + 1$ (by Hadamard's inequality)
    - And not guaranteed if $t < 2\alpha + 1$

Our Idea

- Use not only the shortest vector $\vec{v}$, but **also the second shortest basis vector $\vec{u}$** (both obtained by Gaussian reduction at once)
  - $\vec{q} = (q_1, q_2)$ can be written as $\vec{q} = a\vec{v} + b\vec{u}$, $a, b \in \mathbb{Z}$
  - If **(**)** $|\boldsymbol{a}|, |\boldsymbol{b}| \leq \boldsymbol{poly}(\boldsymbol{\kappa})$, then a, b (hence $\vec{q}$) are found in time $poly(\kappa)$
  - $\vec{q} = a\vec{v} + b\vec{u}$ implies $|a|, |b| = \frac{|(\text{quadratic in } q_i, v_i, u_i)|}{|\det(\vec{v}, \vec{u})|} \leq (\text{const}) \cdot Q^2/T$
    - Where we used $|\det(\vec{v}, \vec{u})| = |\det((1, N_2/N_1 \; mod \; T), (0, T))| = T$ (property of Gaussian reduction) and $||\vec{v}|| \leq ||\vec{u}|| \leq ||\vec{q}|| \leq Q$
      - The other case $||\vec{q}|| < ||\vec{u}||$ is as in the previous work
  - Hence (**) is guaranteed when $Q^2/T = poly(\kappa)$ (or $2\alpha - t = O(\log \kappa)$)

Our Proposed Algorithm

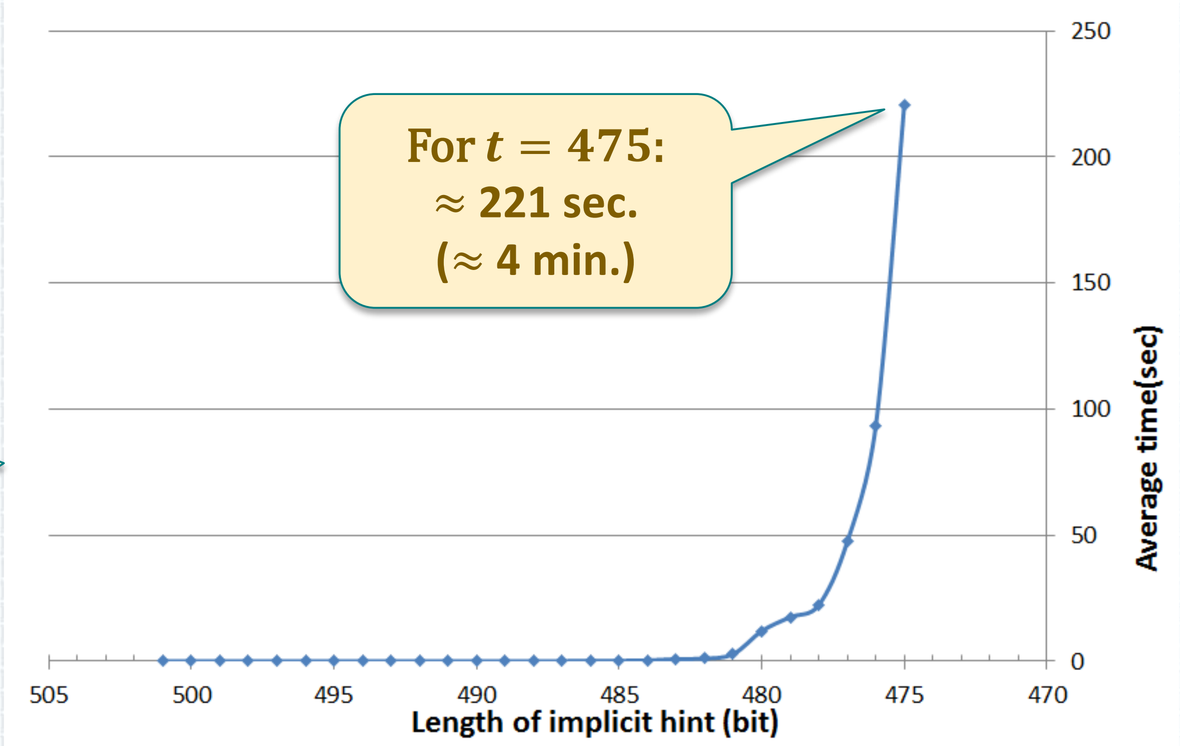
1. Compute $\vec{v}, \vec{u}$ from $(1, N_2/N_1 \; mod \; T), (0, T)$ by Gaussian reduction
2. Output common factors of N_i and v_j (or u_j), if exists
3. For $A = 2, 3, \ldots$, do the following
    1. For integers a, b satisfying $|a| + |b| = A$, do the following
        1. If $|av_1 + bu_1|$ is a non-trivial factor of N_1, output it

Computer Experiments: Average Time

- $\alpha = 250$
- Range of t: $501 = 2\alpha + 1$ to 475
- Ordinary PC
- 100 trials each

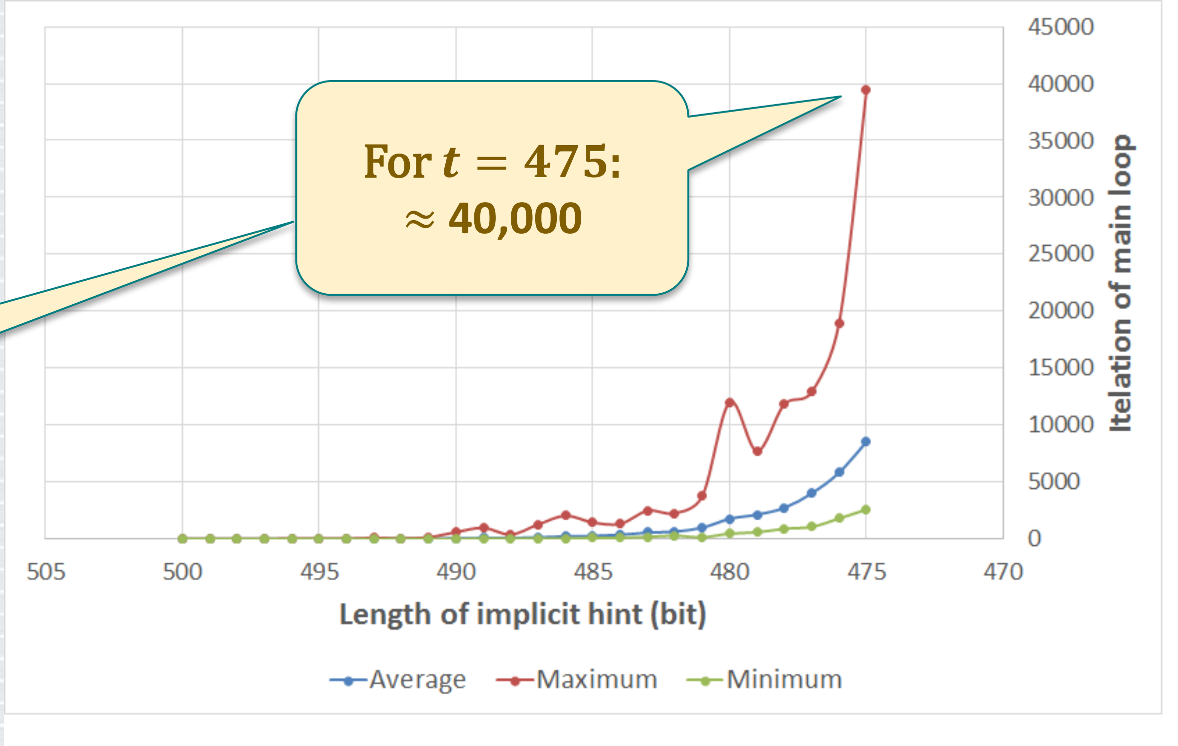
100% Success

(cf., in [KU13]: 40% for $t = 500$ 0% for $t = 499$)



Computer Experiments: # of Iterations

- $\alpha = 250$
- Range of t:
  $501 = 2\alpha + 1$ to 475
- Ordinary PC
- 100 trials each



Bound by our argument:

$\leq 2^{2\alpha+2-t}$

$= 2^{27} \approx 1.34 \times 10^8$

(Probably too loose)

RSA Conference2015

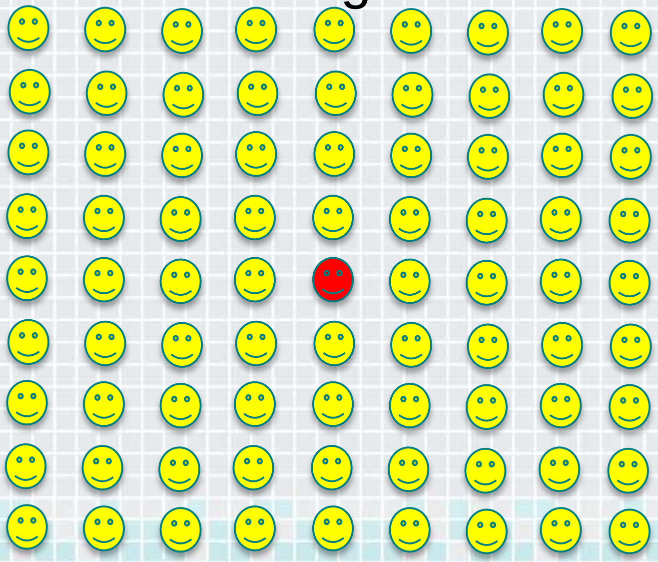
San Francisco | April 20-24 | Moscone Center

#RSAC

Summary

Summary and Future Work

- Improvement of a known factoring algorithm with implicit hints
  - Better bound, even by a simpler proof
- (Potential) applications; e.g., (batch) FHE over integers
- Future work:
  - Sharper analysis of bounds?
  - More applications?



Thank you
for your attentions!