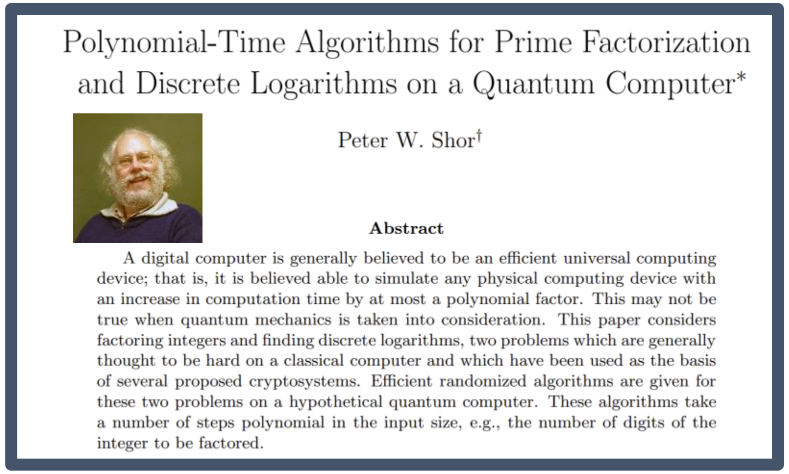
CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Crypatanalysis of some Lattice-based Assumptions

Dipayan Das (joinning NTT Japan in December)

Lattice-based cryptography



Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

- Post-quantum candidate.
- Worst-case to average-case reductions (in asymptotic sense) .
- Advanced cryptographic primitives (like FHE).

NIST standardized lattice-based algorithms for quantum-resistant cryptography (July, 2022).

More details, please visit:

https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

The availability of a quantum computer is altogether a different question ☺

Lattice-based assumptions

Cryptography relies on the assumptions of computationally hard problems.

Lattice-based assumptions: The best known way to solve it is by lattice methods through a transformation to a lattice problem.

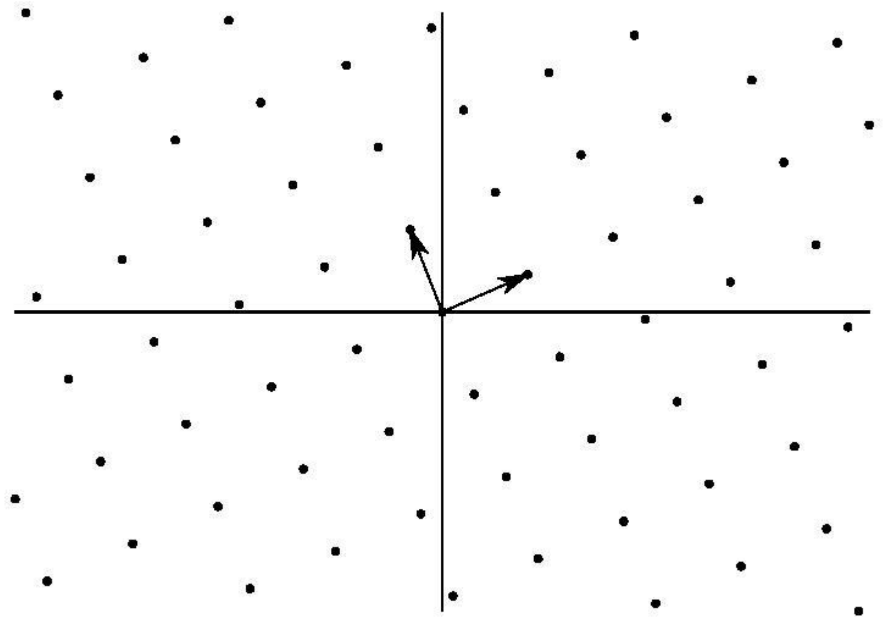
Talk overview: This doesn't always guarantee hardness (by counterexamples).

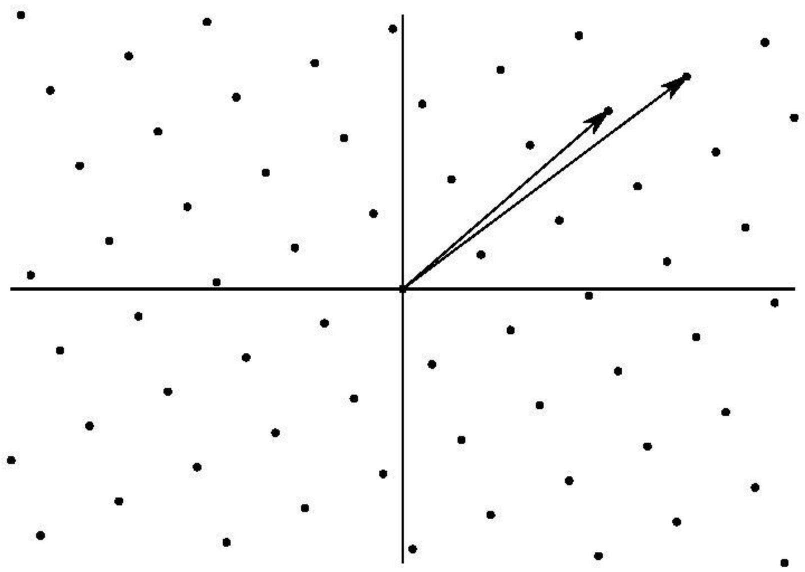
Lattice methods might not be the optimal strategy to approach it.

Lattice Background

A full rank matrix $\mathrm{B} \in \mathbb{Z}^{n\times n}$ generates a ***Lattice*** $L = L(B) = \{Bz: z \in \mathbb{Z}^n\}$

- This lattice has $dim = n$ and $Vol = |det(B)|$





Algorithmic problem related to lattices

- Shortest (non-zero) vector problem (SVP)
- Minkowski's theorem: Let v be the SVP solution, then

$$|| v|| \leq \sqrt{n} Vol^{\frac{1}{n}}$$

- In practice, we use lattice reduction algorithms to find approximate solutions.

LLL: Finds a lattice vector of norm $\leq 2^{\frac{n}{2}}\, Vol^{\frac{1}{n}}$ in polynomial time in the size of its input.

BKZ with block size β: Finds a lattice vector of norm $\leq \beta^{\frac{n}{\beta}} Vol^{\frac{1}{n}}$ in time $2^{O(\beta)}$.

Cryptanalysis of the Finite Field Isomorphism problem

Based on the work: D. Das, A. Joux. On the Hardness of the Finite Field Isomorphism Problem. EUROCRYPT'23

Reminders from Finite field theory

- Finite field with q elements : F_q , where q is prime.

- Finite field with q^n elements (n degree extension of F_q): F_{q^n}

- Isomorphic representations of $\mathrm{F}_{\mathrm{q}^n}$ using irreducible polynomials of degree n over F_q

$$F_q[x]/f(x) \approx F_q[y]/F(y) \approx \ldots$$

- To find an explicit isomorphism, it is enough to know the roots of one polynomial in F_{q^n} in terms of the other representation

Finite Field Isomorphism (FFI) Distribution

Private:	**Public:**
Uniform Sparse ternary minimal polynomial of x: $f(x) = x^n + g(x)$, $\deg(g) \leq \frac{n}{2}$	Uniform minimal polynomial of y: $F(y)$
Pick an Isomorphism: ϕ	
Sample β- bounded linear combinations of powers of x: $a_i(x)$	$A_i(y) = \phi(a_i(x))$

Good Representation in polynomial x —basis

Bad Representation in polynomial y —basis

FFI problem [DHP+'18,HSWZ'20]

Given $q, F(y), A_1(y), A_2(y), \ldots, A_k(y)$ **decide** if $A_i(y)$ is from the FFI distribution **or** the uniform distribution.

This is the Decisional FFI (DFFI) problem.

[DHP+'18]: Y. Doröz, J. Hoffstein, J. Pipher, J. Silverman, B. Sunar, W. Whyte, and Z. Zhang. Fully homomorphic encryption from the finite field isomorphism problem. PKC'18.

[HSWZ'20]: J. Hoffstein, J. Silverman, W. Whyte, Z. Zhang. A signature scheme from the finite field isomorphism problem. JoMC'20.

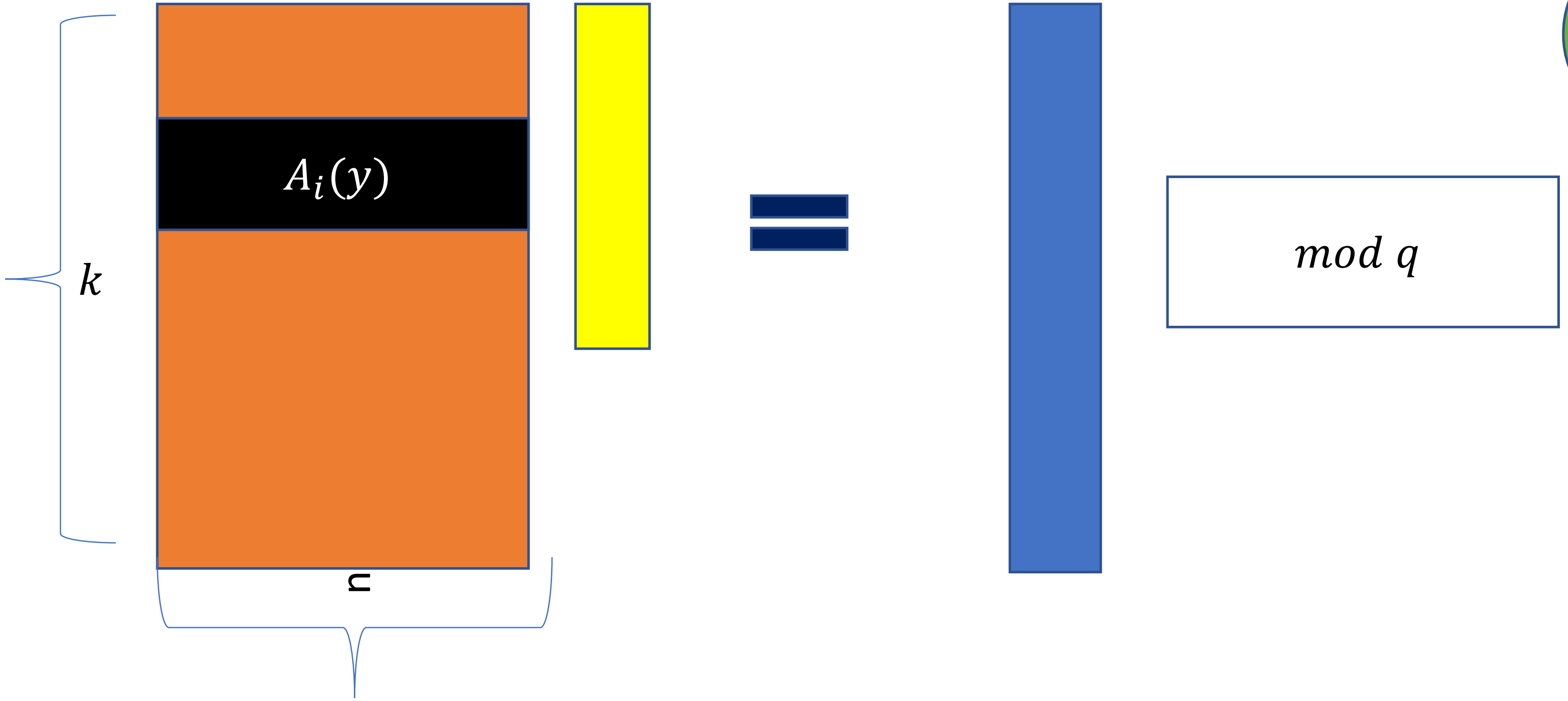
Toy example

```
n=16
q=32771

f(x)=x^16 + x^7 + x^5 -x^3 - x^2 -x + 1

F(y)=y^16 + 4152*y^15 + 2594*y^14 + 26843*y^13 + 27498*y^12 + 31444*y^11
+ 15956*y^10 + 7616*y^9 + 30326*y^8 + 26729*y^7 + 8558*y^6 + 4785*y^5 +
27721*y^4 + 1198*y^3 + 14942*y^2 + 14544*y + 11277

\phi= 28228*y^15 + 13643*y^14 + 21168*y^13 + 4909*y^12 + 25475*y^11 +
21646*y^10 + 23297*y^9 + 19665*y^8 + 5019*y^7 + 1677*y^6 + 6823*y^5 +
15399*y^4 + 23882*y^3 + 242*y^2 + 18578*y + 31824

x-basis representataions
y-basis representations


x^14 + x^12 + x^10 + x^9 + x^8 -x^7 -x^6 -x^5 -x^4 -x^3 -x


28795*y^15 + 757*y^14 + 4649*y^13 + 30560*y^12 + 21773*y^11 + 19702*y^10
+ 14924*y^9 + 22488*y^8 + 29775*y^7 + 7212*y^6 + 5478*y^5 + 4488*y^4 +
9598*y^3 + 3290*y^2 + 19954*y + 25737


x^13 -x^12 + x^10 -x^9 + x^7 + x^5 -x^4 + x^3 -x^2 -x + 1


22173*y^15 + 15726*y^14 + 3731*y^13 + 2685*y^12 + 29516*y^11 + 30642*y^10
+ 9001*y^9 + 12333*y^8 + 8722*y^7 + 3340*y^6 + 28353*y^5 + 9853*y^4 +
32035*y^3 + 25337*y^2 + 19076*y + 29241


-x^15 + x^12 -x^11 -x^10 + x^8 -x^6 -x^5 -x^3 -x^2 -*x -1


25606*y^15 + 24744*y^14 + 20203*y^13 + 1563*y^12 + 10690*y^11 +
20096*y^10 + 22744*y^9 + 30083*y^8 + 16058*y^7 + 10331*y^6 + 30479*y^5 +
27544*y^4 + 19920*y^3 + 3869*y^2 + 6833*y + 2377
```

Previous attack on Decisional FFI problem [DHP+'18,HSWZ'20]

Lattice attack

Find unusually short lattice vectors of the lattice $L \subseteq \mathbb{Z}^k$ spanned by the columns



FHE from FFI problem (oversimplified) [DHP+'18]

- Let $p = 2$
- $m_a, m_b \in \{0,1\}$
- Enc$(m_a) = C_a = pC(y) + m_a$, Enc$(m_b) = C_b = pC'(y) + m_b$
- Dec$(C_a) = (pc(x) + m_a)\ mod\ p = m_a$
- Dec$(C_a + C_b) = (p\ c(x) + pc'(x) + m_a + m_b\ )mod\ p = m_a + m_b$
- Dec$(C_a . C_b) = (p^2\ c(x)c'(x) + p\ c(x)m_b + pc'(x)m_a + m_a . m_b)\ mod\ p = m_a . m_b$
- Correctness: Choose q sufficiently large to avoid modular reductions in x-basis representations
- When $q = 2^{n^\delta}, \delta \in (0,1)$, the Encryption scheme is FHE [DHP+18]

Bounded Expansion factor
The sparse ternary choice of $f(x)$ bounds the noise growth after multiplications

Trace of finite field

- Let $\alpha \in F_{q^n}$, trace is defined by

$$Tr(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}} \in F_q$$

- Trace is linear.
- Trace computation is polynomial time.
- Trace is invariant under basis representations.

Symmetric polynomials

- Roots of $f(x)$ in F_{q^n}(in terms of polynomial x-basis):

$$\{\alpha_0 = x, \alpha_1 = x^q, \dots, \alpha_{n-1} = x^{q^{n-1}}\}$$

- Define Symmetric polynomials

$$\sigma_1(\alpha_i) = -\sum \alpha_i, \sigma_2(\alpha_i) = \sum\sum \alpha_i \alpha_j, \dots, \sigma_n(\alpha_i) = (-1)^n \prod \alpha_i$$

Trace of polynomial x-basis

$$f(x) = x^n + \sigma_1 x^{n-1} + \cdots + \sigma_n \text{ where } \sigma_d = 0 \text{ for } 1 \le d \le \frac{n}{2} - 1$$

$$\sigma_d \in \{0, \pm 1\} \text{ for } \frac{n}{2} \le d \le n$$

Then

$$\begin{aligned} \left|Tr\left(x^d\right)\right| &= n \, mod \, q \quad \text{for } d = 0 \\ &= 0 \, mod \, q \quad \text{for } 1 \le d \le \frac{n}{2} - 1 \\ &= d \, mod \, q \quad \text{for } \frac{n}{2} \le d \le n-1 \text{ and } \sigma_d \ne 0 \\ &= 0 \, mod \, q \qquad \sigma_d = 0 \end{aligned}$$

Trace of polynomial x-basis

$f(x) = x^n + \sigma_1 x^{n-1} + \cdots + \sigma_n$ where $\sigma_d = 0$ for $1 \leq d \leq \frac{n}{2} - 1$

$\sigma_d \in \{0, \pm 1\}$ for $\frac{n}{2} \leq d \leq n$

- Then for $1 \leq d \leq \frac{n}{2} - 1$
- $\sigma_d = 0$
- $Tr(x^d) = 0 \; mod \; q$

Using Newton-Girard formula:

$$Tr(x^d) = (-1)^d d \sum_{r_i \in \mathbb{N}: r_1 + 2r_2 + \cdots + d r_d = d} \frac{(r_1 + r_2 + \cdots r_d - 1)!}{r_1! \, r_2! \ldots r_d!} \prod_{j=1}^{d} (-\sigma_j)^{r_j}$$

Trace of polynomial x-basis

$$f(x) = x^n + \sigma_1 x^{n-1} + \cdots + \sigma_n \text{ where } \sigma_d = 0 \text{ for } 1 \le d \le \frac{n}{2} - 1$$

$$\sigma_d \in \{0, \pm 1\} \text{ for } \frac{n}{2} \le d \le n$$

- Then for $\frac{\mathrm{n}}{2} \le d \le n - 1$

Only one solution for $r_i: r_1 + 2r_2 + \cdots + dr_d = d$ that contributes in the sum:

$$(r_1 = 0, r_2 = 0, \dots, r_d = 1)$$

$$|Tr(x^d)| = d \bmod q \text{ when } \sigma_d \neq 0$$

$$= 0 \bmod q \text{ when } \sigma_d = 0$$

Using Newton-Girard formula:

$$Tr(x^d) = (-1)^d d \sum_{r_i \in \mathbb{N}: r_1 + 2r_2 + \cdots + dr_d = d} \frac{(r_1 + r_2 + \cdots r_d - 1)!}{r_1! \, r_2! \dots r_d!} \prod_{j=1}^{d} (-\sigma_j)^{r_j}$$

Trace of FFI samples

- Let $a_i(x)$ is a β-linear combinations of x-basis.

Then $\left|Tr\left(a_i(x)\right)\right| = \left|Tr\left(A_i(y)\right)\right| \leq \beta n^2$

Polynomial-time attack on DFFI problem

- Let $q > 4\beta n^2$
- Let $A_1(y), A_2(y), \ldots, A_k(y)$ be the given samples.

Compute the trace of the samples.

If the absolute value of traces $\leq \beta n^2$, output FFI distribution.

Otherwise, output uniform distribution.

- Advantage: $1 - \frac{1}{2^k}$

Trace is uniformly distributed in F_q for uniform samples.

Polynomial-time semantic attack on the FHE

- Let p is not a divisor of n
- $C_a = pC(y) + m$, where $m \in \{0,1\}$
- $Tr(C_a) = pTr(c(x)) + Tr(m)$ is small.

$Tr(C_a) mod\ p = 0$, Return $m = 0$
$= 1$, Return $m = 1$

Polynomial-time semantic attack on the FHE

- Let p is a divisor of n
- $C_a \;= pC(y) + m$, where $m \in \{0,1\}$
- Pick any FFI sample C^* such that p is not a divisor of $Tr(C^*)$
- $Tr(C_a . C^* \,) = pTr(c^*(x). c(x)) + m\, Tr(c^*(x))$ is still small.

The choice of $f(x)$ makes sure the coefficients of the product in x-basis are small.

$$
\begin{aligned}
Tr(C_a C^*) mod\, p &= 0, \text{Return } m = 0 \\
&= 1, \text{Return } m = 1
\end{aligned}
$$

- The large q makes sure there is no modular reduction!

Cryptanalysis of the Partial Vandermonde Knapsack Problem

Based on the work: D. Das, A. Joux. Key Recovery Attack on the Partial Vandermonde Knapsack Problem. In submission

Partial Vandermonde (PV) Knapsack Problem

Let $R_q = F_q[x]/g(x)$ be a quotient polynomial ring, where

- $g(x) = x^n - 1$ for prime n
  $= x^n + 1$ for power of two n
- Prime q such that $g(x)$ splits linearly over F_q

When n is prime, $q = 1 \; mod \; n$

When n is power-of-two, $q = 1 \; mod \; 2n$

Ω: The set of all the primitive roots of $g(x)$ over F_q

PV Knapsack Problem [HPSSW'14,HS'15,DHSS'20, LZA'18,BSS'22]

- Ω_t: Uniformly random subset of Ω with t distinct elements.
- $f(x) \in R_q$: Coefficients are sampled uniformly at random from the set $\{-1,0,1\}$.

PV Knapsack problem:

Given R_q, Ω_t, and $f(\omega)$ for $\omega \in \Omega_t$ find $f(x)$ when $t \approx \frac{n}{2}$.

Initially PV Knapsack problem was called the partial Fourier recovery problem.

[HPSSW'14]: J. Hoffstein, J. Pipher, J. Schanck, J. Silverman, and W. Whyte. Practical signatures from the partial Fourier recovery problem. ACNS'14.

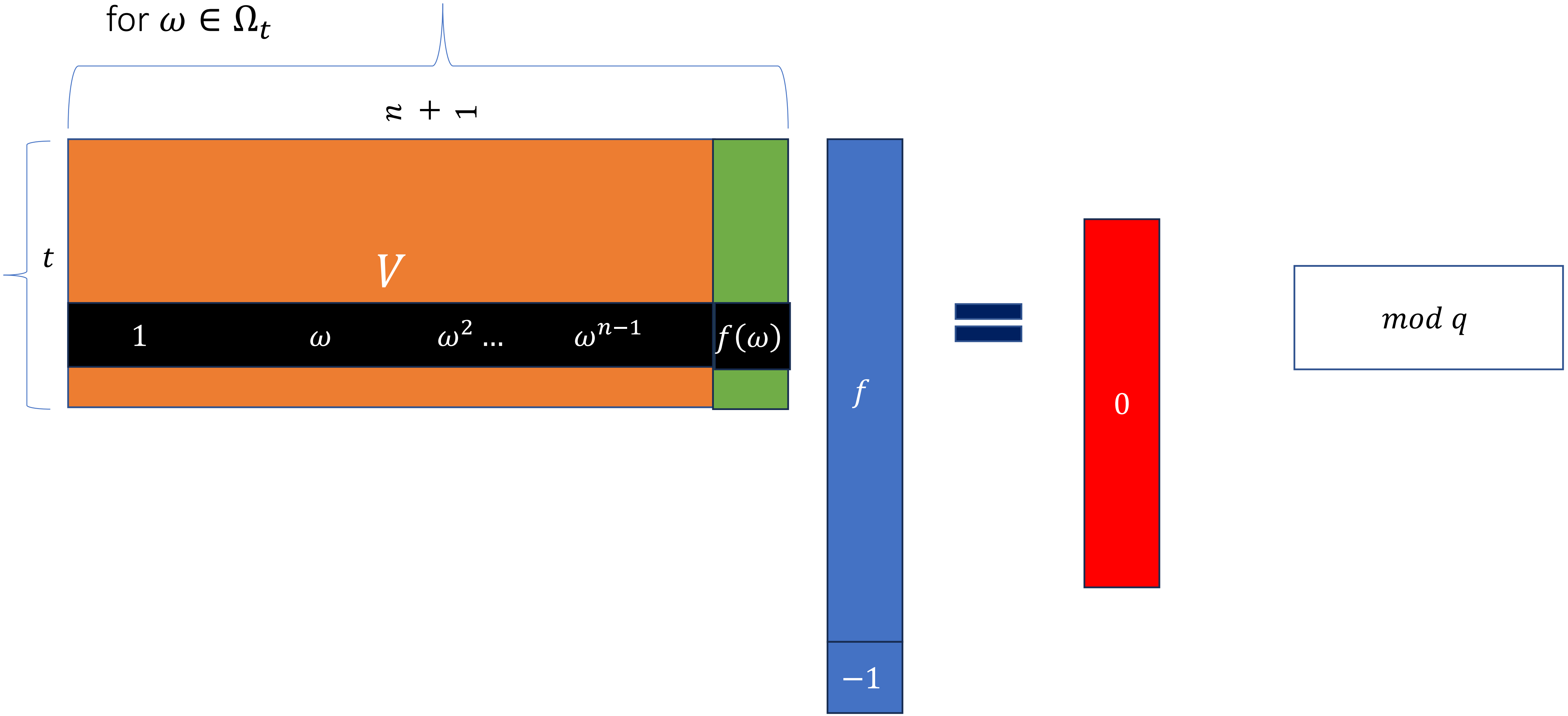
[HS'15]: J. Hoffstein and J. Silverman. Pass-encrypt: a public key cryptosystem based on partial evaluation of polynomials. DCC'15.

[LZA'18]: X. Lu, Z. Zhang, and M. Au. Practical signatures from the partial Fourier recovery problem revisited: A provably-secure and Gaussian-distributed construction. ACISP'18.

[DHSS'20]: Y. Doröz, J. Hoffstein, J. Silverman, and B. Sunar. MMSAT: A scheme for multimessage multiuser signature aggregation. Eprint'20.

[BSS'22]: K. Boudgoust, A. Sakzad, and R. Steinfeld. Vandermonde meets Regev: public key encryption schemes based on partial Vandermonde problems. DCC'22.

Previous attack (Direct primal attack)[HPSSW'14]



Previous attack (Direct primal attack)[HPSSW'14]

- PV Knapsack problem: Find the uSVP solution $(f, -1)$ on the Kernel lattice

$$L^{\perp} = \{x \in \mathbb{Z}^{n+1} : Vx = 0 \; mod \; q\}$$

With $Dim = n + 1 \quad Vol = q^t$

- $||\,(f, -1)\,|| \approx \sqrt{\frac{2n}{3}}$ which is unusually short in the lattice $L^{\perp}$.

Previous attack (Dual attack)[BGP'22]

- Distinguishing attack
- Doesn't affect the hardness of recovering f.

"*We note however that this does not fully invalidate the claim made in [LZA18], since the 128 bit-security is claimed against search attackers, and not distinguishing attackers.*" [BGP'22]

- The attack exploits specific Ideal structure of the problem to map to an SVP instance of smaller dimension.

[BGP'22]: K. Boudgoust, E. Gachon, and A. Pellet-Mary. Some easy instances of Ideal-SVP and implications on the partial Vandermonde Knapsack problem. Crypto'22.

Attack on the PV Knapsack problem

- For any $f(x) \in R_q$, we can interpret $f\left(\frac{1}{x}\right) \in R_q$

- $\frac{1}{x} = x^{n-1} \in R_q$ when n is prime.
- $\frac{1}{x} = -x^{n-1} \in R_q$ when n is power-of-two.

Attack on the PV Knapsack problem

- Consider $\Omega_{2t_1} = \{\omega \in \Omega_t : (\omega, \omega^{-1}) \in \Omega_t\} \subseteq \Omega_t$ with $0 \leq t_1 \leq \lfloor \frac{t}{2} \rfloor$
- We know the evaluations $f(\omega)$ and $f(\omega^{-1})$
- We can compute $f(\omega) \pm f(\omega^{-1})$ for $\omega \in \Omega_{2t_1}$

This gives t_1 evaluations of $\psi_{\pm}(x) = f(x) \pm f\left(\frac{1}{x}\right)$ at $\omega \in \Omega_{2t_1}$

Idea: Find $\psi_{\pm}(x)$ using lattice of smaller dimensions and do linear algebra to recover $f(x)$. Finding each of $\psi_{\pm}(x)$ can be performed in parallel.

Attack on the PV Knapsack problem

- The mapping

  $x^i \to x^i + 1/x^i$ for $0 \le i \le \lfloor \frac{n}{2} \rfloor$ is well defined.

By linearity, $\psi_+(x) = f(x) + f\left(\frac{1}{x}\right)$ can be generated by the basis (of order $\lceil \frac{n}{2} \rceil$)

$$\left\{2, \left(x + \frac{1}{x}\right), \left(x^2 + \frac{1}{x^2}\right), \dots, \left(x^{\left\lfloor \frac{n}{2} \right\rfloor} + \frac{1}{x^{\left\lfloor \frac{n}{2} \right\rfloor + 1}}\right)\right\}$$

Similarly, $\psi_-(x) = f(x) - f\left(\frac{1}{x}\right)$can be generated by the basis (of order $\lfloor \frac{n}{2} \rfloor$)

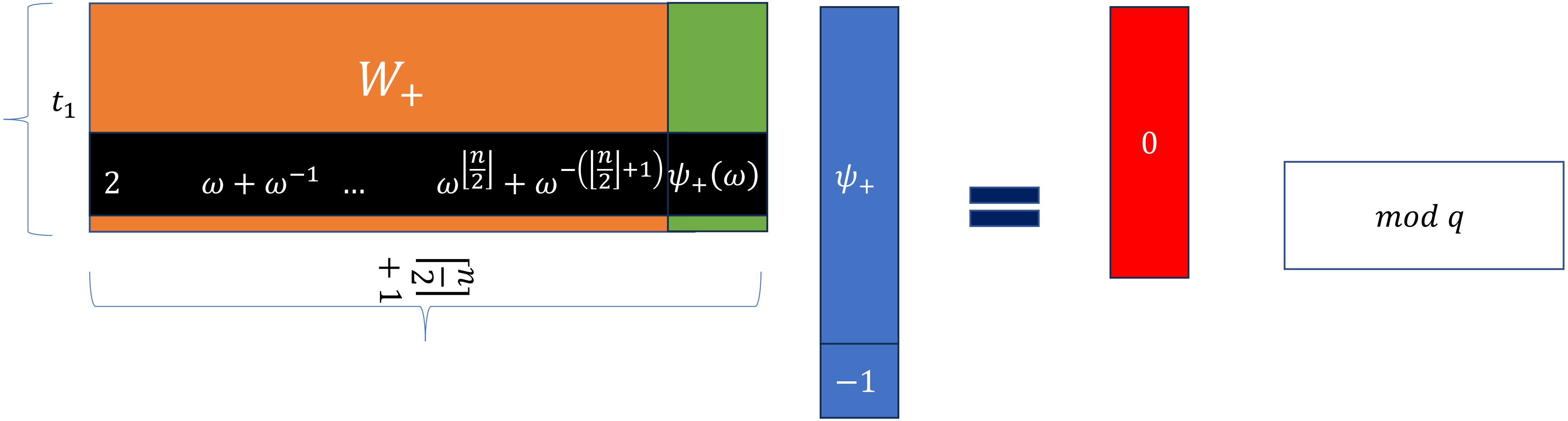
$$\left\{\left(x - \frac{1}{x}\right), \left(x^2 - \frac{1}{x^2}\right), \dots, \left(x^{\left\lfloor \frac{n}{2} \right\rfloor} - \frac{1}{x^{\left\lfloor \frac{n}{2} \right\rfloor + 1}}\right)\right\}$$

- If $f(x)$ has uniformly random coefficients in $\{-1,0,1\}$, $\psi_\pm(x)$ has coefficients in $\{-2,-1,0,1,2\}$ and

$||\psi_\pm|| \approx \sqrt{\frac{4\lceil \frac{n}{2} \rceil}{3}}$ in the new basis representations.

Attack on the PV Knapsack problem

for $\omega \in \Omega_{2t_1}$



New Primal Attack on the PV Knapsack problem

PV Knapsack problem reduced to finding the uSVP solution on the Kernel lattice

$$L_{W_+}^{\perp} = \{x \in \mathbb{Z}^{\lceil \frac{n}{2} \rceil +1} : W_+ x = 0 \; mod \; q \}$$

With $Dim = \lceil \frac{n}{2} \rceil + 1 \quad Vol = q^{t_1}$

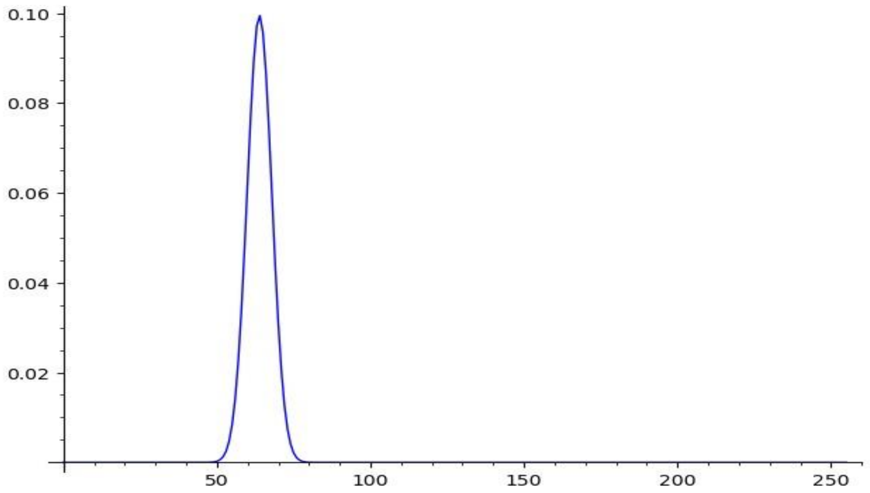
$||(\psi_{\pm}, -1)|| \approx \sqrt{\frac{4\lceil \frac{n}{2} \rceil}{3}}$ which is also unusually short in the lattice $L_{W_{\pm}}^{\perp}$.

Analysis of the attack

- uSVP cost depends on the root Hermite factor $\delta = \gamma^{1/dim}$, $\gamma = \frac{\lambda_2}{\lambda_1}$ is the uniqueness gap [GN'08].
- The attack gets faster as t_1 increases.

Probability distribution of the number of pairs t_1:

$$\pi_1(t_1) = \frac{\binom{\lfloor \frac{n}{2} \rfloor}{t_1}\binom{\lfloor \frac{n}{2} \rfloor - t_1}{t - 2t_1} 2^{t-2t_1}}{\binom{2\lfloor \frac{n}{2} \rfloor}{t}}$$



$\pi_1(t_1)$ for $n = 512, t = 256$

[GN'08]: N. Gama and P. Nguyen. Predicting lattice reduction. Eurocrypt'08.

Effect of the attack on the concrete parameters

All the parameters from the literature contain a non-negligible fraction of weak keys, which are easily identified and extremely susceptible to our attack.

Example: We recovered the secret key of a parameter set from [LZA'18] for a fraction of

- 2^{-15} of the public keys in about 117 hours ($\approx 2^{50}$ bits operation)
- 2^{-19} of the public keys in about 30 hours ($\approx 2^{48}$ bits operation)
- 2^{-23} of the public keys in about 10 hours ($\approx 2^{46}$ bits operation)
- 2^{-30} of the public keys in about 8 hours ($\approx 2^{45}$ bits operation)

The direct primal attack provides 54-bits security using LWE estimator [APS'15].

It was initially claimed to have a 128-bit security against key recovery attack [LZA18], which was reduced to 87-bit security using the distinguishing attack from [BGP'22].

[APS'15] M. Albrecht, R. Player, and S. Scott. On the concrete hardness of learning with errors. JoMC'15.

Conclusion

“40 years Advances in Cryptology: How will future judge Us?”

Crypto’20 Rump talk by Yvo Desmedt available at https://www.youtube.com/watch?v=MTafClFZOi8&list=PLeeS-3Ml-rppZMjRn2bNhb1FU-JOLMjRU&index=36&t=4650s

- Lattice-based assumptions are “relatively” NEW.

- CRYPTANALYSIS challenges our assumptions.