Key Recovery Attack on the Partial Vandermonde Knapsack Problem

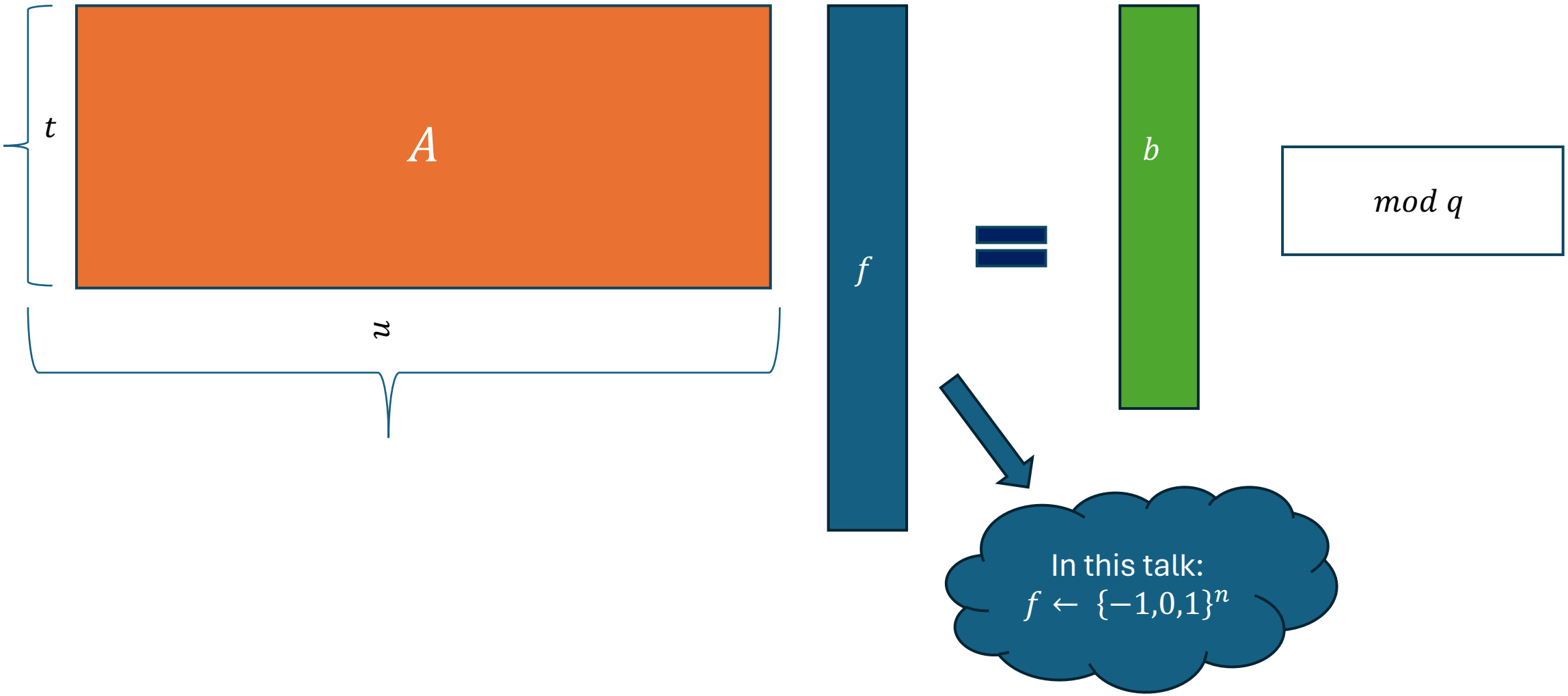
Dipayan Das

NTT Social Informatics Laboratories, Tokyo, Japan

Antoine Joux

CISPA Helmholtz Center for Information Security, Saarbrücken, Germany

Low-density ISIS (or LWE) problem



Practical lattice-based assumptions

- For efficiency, use algebraic variants of A.

- Partial Vandermonde (PV) Knapsack Problem: An algebraic variant of the low-density ISIS problem.

This talk: A non-negligible fraction of the PV Knapsack keys proposed in the literature are weak.

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.

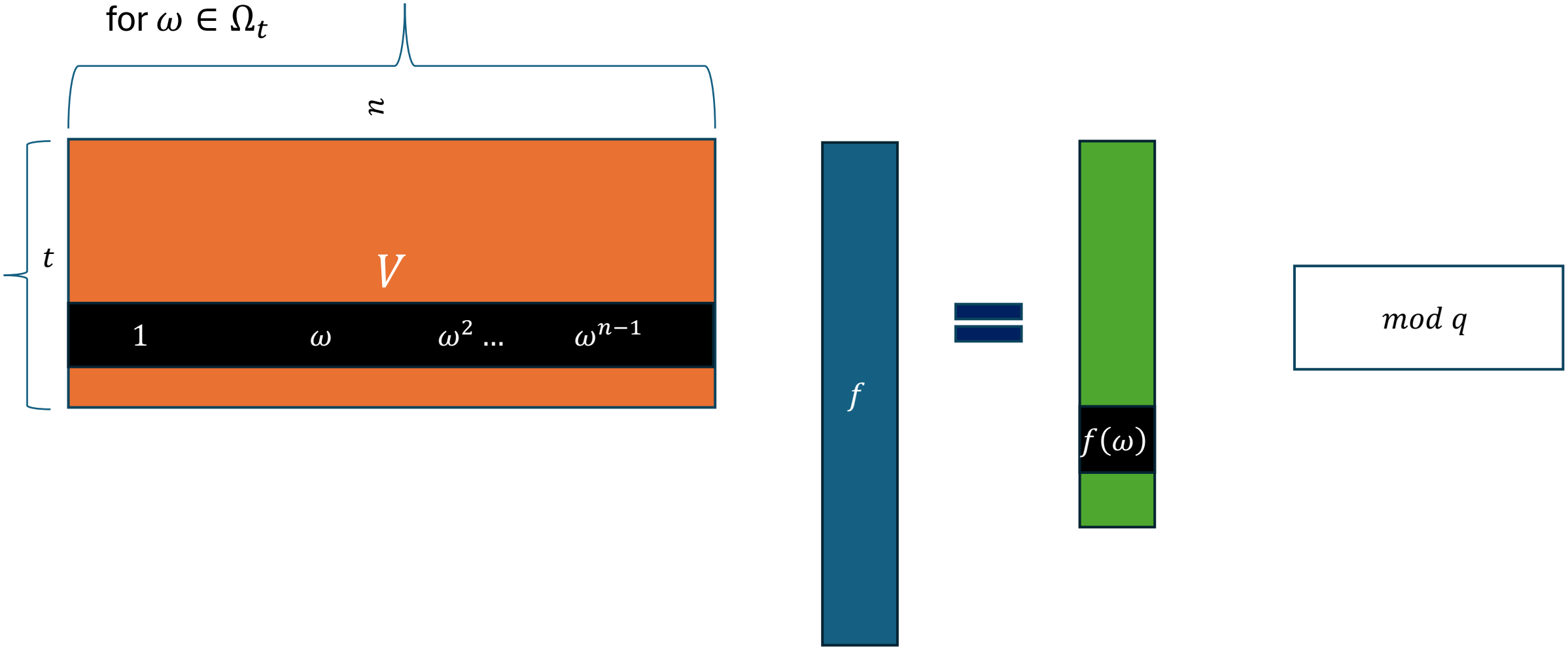
[HS'15]: J. Hoffstein and J. Silverman. Pass-encrypt: a public key cryptosystem based on partial evaluation of polynomials. DCC'15.

[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.

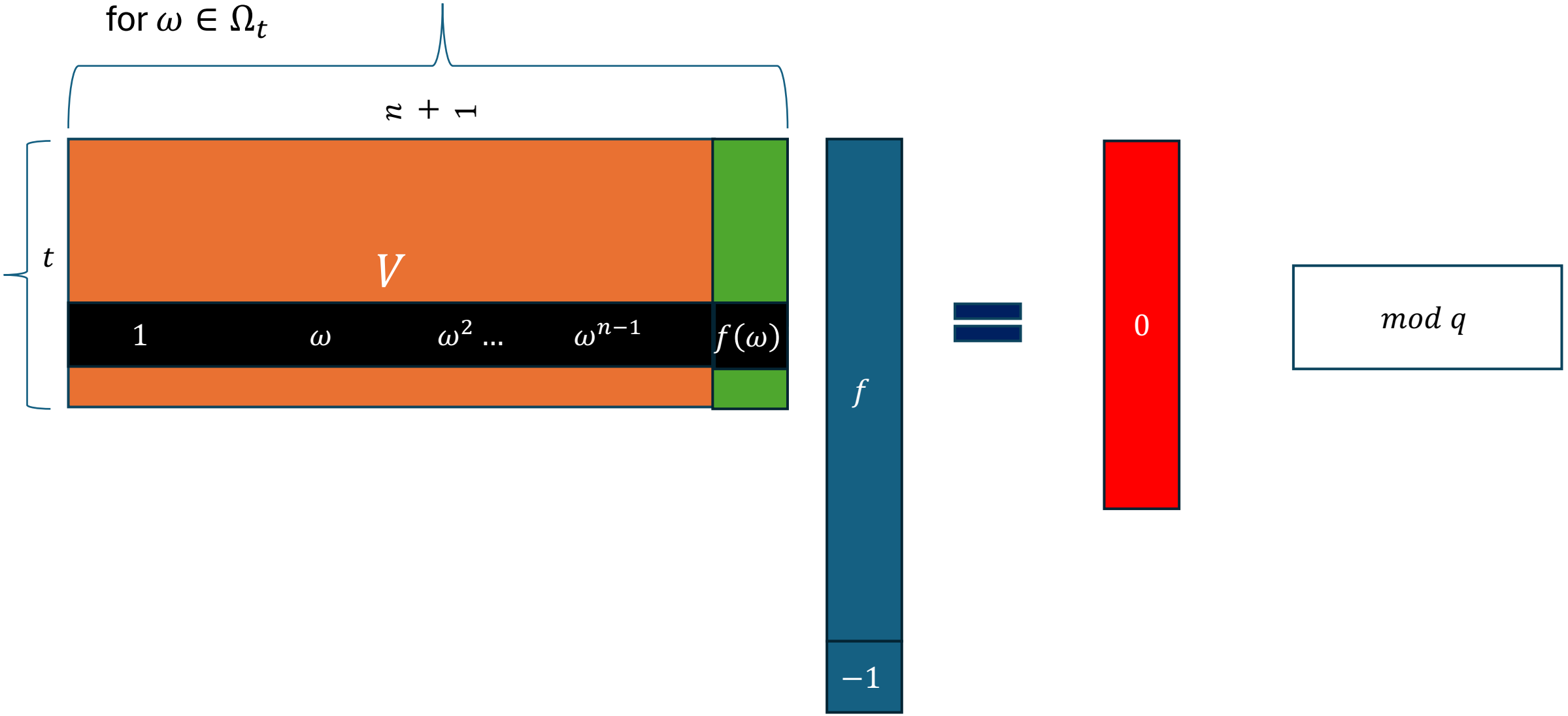
[DHSS'20]: Y. Doröz, J. Hoffstein, J. Silverman, and B. Sunar. MMSAT: A scheme for multimessage multiuser signature aggregation. Eprint'20.

[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]

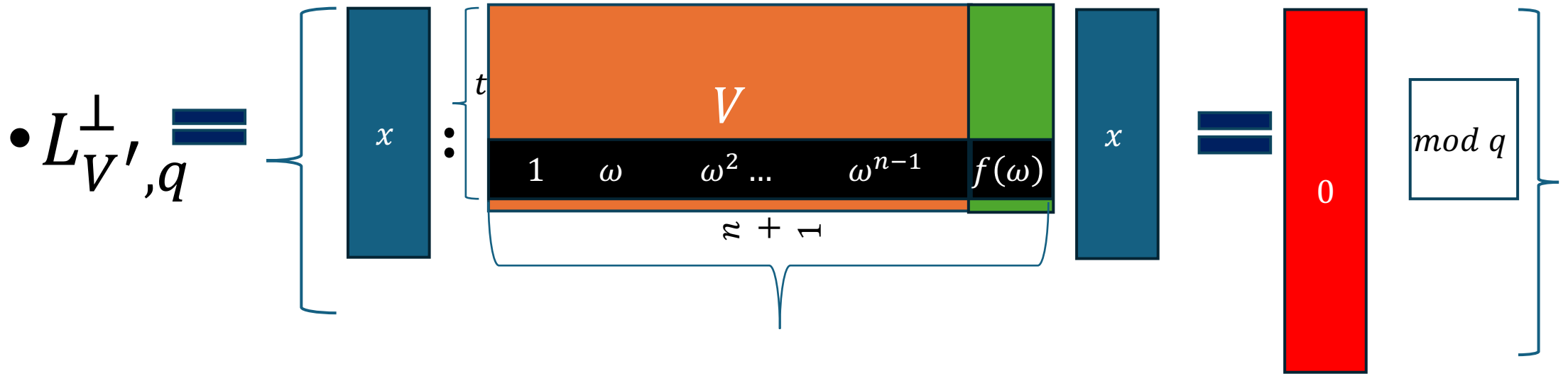


Previous attack (Direct primal attack)[HPSSW'14]



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

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



With lattice dimension $\dim = n + 1$, volume $\mathrm{Vol} = q^t$.

- $(f, -1)^T \in L^{\perp}_{V',q}$, $\|(f, -1)^T\| = O(\sqrt{n})$ which is **unusually short** in the lattice $L^{\perp}_{V',q}$.

Minkowski's theorem: The shortest vector $v \in L^{\perp}_{V',q}$: $\|v\| \leq \sqrt{n+1}Vol^{\frac{1}{n+1}} \approx \sqrt{(nq)}$ when $t \approx \frac{n}{2}$.

Previous attack (Dual attack, simplified version)[BGP'22]

key distinguishing attack

Let z be any solution such that $Vz = b \; mod \; q$

Then, for a PV Knapsack instance, $\exists \; u \in L^{\perp}_{V,q}$ such that $u - z = f$

Algebraically, $u(x) \in I_{\Omega_t}$ where $I_{\Omega_t} = \prod_{\omega \in \Omega_t} (x - \omega) \subset R_q$

Let $u'(x) \in I_{\Omega \setminus \Omega_t} = \prod_{\omega \in \Omega / \Omega_t} (x - \omega)$ with "somewhat" small norm, then

- For PV Knapsack instance,

  $u'(x)z(x) = u'(x)f(x) \in R_q$ is expected to have a small norm.

- For uniform instance, a highly unlikely event.

[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.

Dual attack (simplified version)[BGP'22]

- The cost of the attack depends on finding $u'(x) \in I_{\Omega \setminus \Omega_t}$ with small norm.
- Let $\Omega_{2t_1} = \{\omega \in \Omega_t : (\omega, \omega^{-1}) \in \Omega_t\} \subseteq \Omega_t$ with $0 \leq t_1 \leq \lfloor \frac{t}{2} \rfloor$.

  Then $\Omega \setminus \Omega_{2t_1}$ is also made of such pairs.
- If t_1 is not too small, PV Knapsack over Ω_t reduces to over Ω_{2t_1}.
- Search for a small $u'(x) \in I_{\Omega \setminus \Omega_{2t_1}}$ satisfying $u'(x) = u'\left(\frac{1}{x}\right)$, which can be generated by the polynomial basis $\left\{1, x, \ldots, x^{\left\lfloor \frac{n}{2} \right\rfloor}\right\}$.

Previous attack (Dual attack)[BGP'22]

- Distinguishing attack in general.
- Doesn't recover the secret f, except for some worst-case keys.

"*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]

- Transforms uSVP instance into SVP instance (in lower dimension).

Key recovery using new primal strategy: We can also exploit the symmetry of the secret $f(x) \in R_q$ to transform uSVP instance into uSVP instance (in lower dimension).

New primal 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 $f(\omega^{-1})$ for $\omega \in \Omega_{2t_1}$.
- We can compute $f(\omega) \pm f(\omega^{-1})$.

This gives t_1 distinct 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 $f(x)$.

New primal attack on the PV Knapsack problem

Let $n_+ = \lceil \frac{n}{2} \rceil, n_- = \lfloor \frac{n}{2} \rfloor$.

For any $f(x) \in R_q$, $\psi_\pm(x) = f(x) \pm f\left(\frac{1}{x}\right)$ can be generated by a basis of order $n_\pm$.

- The mapping

  $x^i \to x^i + 1/x^i$ for $0 \le i \le n_-$ is well defined.

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

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

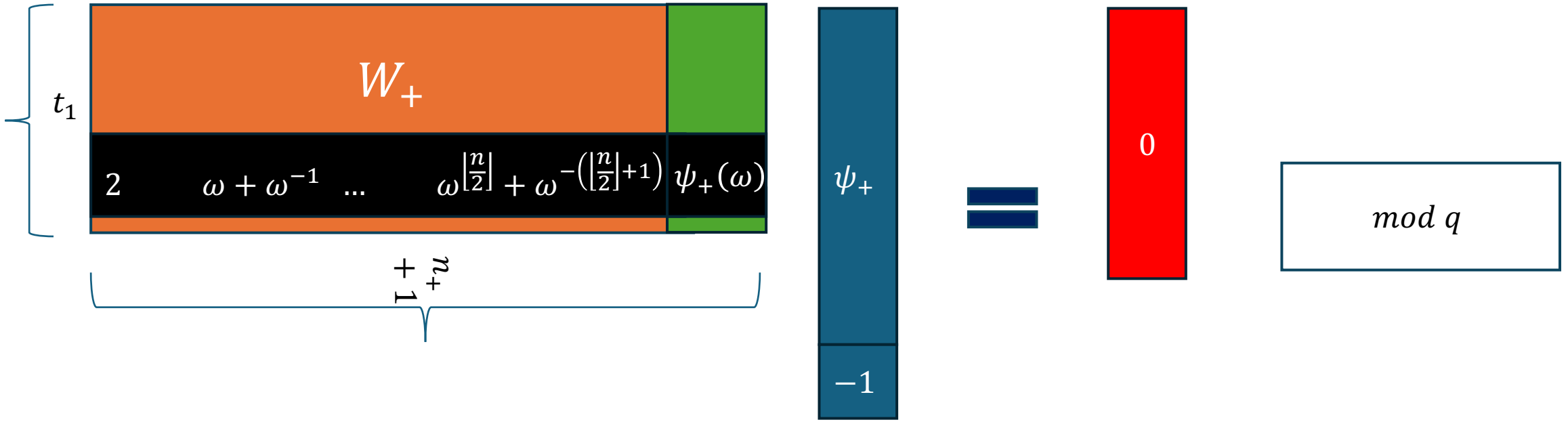
Similarly, $\psi_-(x) = f(x) - f\left(\frac{1}{x}\right)$ can be generated by the basis (of order n_-)

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

- Also, if $f(x)$ has coefficients in $\{-1,0,1\}$, then $\psi_\pm(x)$ has coefficients in $\{-2,-1,0,1,2\}$ and $||\psi_\pm|| = O\left(\sqrt{n_\pm}\right)$ in the new basis representations.

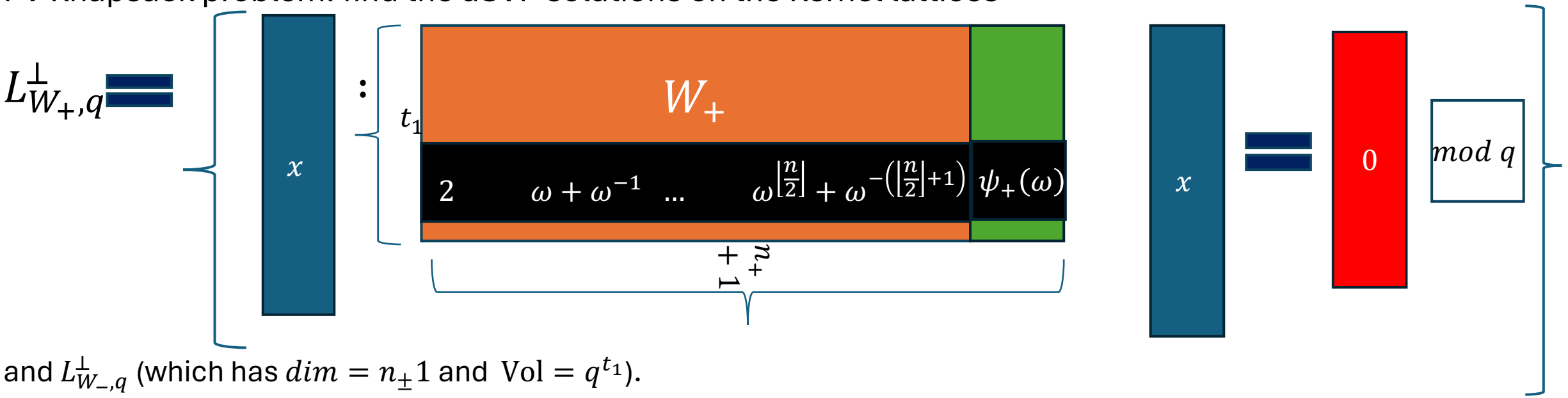
New primal attack on the PV Knapsack problem

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



New primal attack on the PV Knapsack problem

PV Knapsack problem: find the uSVP solutions on the Kernel lattices



and $L^{\perp}_{W_-,q}$ (which has $dim = n_{\pm}1$ and $\mathrm{Vol} = q^{t_1}$).

$(\psi_{\pm}, -1)^T \in L^{\perp}_{W_{\pm},q}, ||(\psi_{\pm}, -1)^T|| = O(\sqrt{n_{\pm}})$ which is also unusually short in the lattice $L^{\perp}_{W_{\pm},q}$.

- Finding each of $\psi_{\pm}$ can be performed in parallel.

Analysis of the new attack

Lattice reduction cost to recover uSVP depends on the root Hermite factor $\delta = \gamma^{1/dim}$, $\gamma = \frac{\lambda_2}{\lambda_1}$ is the uniqueness gap in the lattice [GN'08].

- For the direct primal attack: $\delta_{full} \approx \left(\frac{\sqrt{n}q^{\frac{t}{n}}}{\sqrt{n}}\right)^{\frac{1}{n}}$
- For the new primal attack: $\delta_{new} \approx \left(\frac{\sqrt{n/2}q^{\frac{t_1}{n/2}}}{\sqrt{n/2}}\right)^{\frac{1}{n/2}}$

$\delta_{new} \geq \delta_{full}$ whenever $t_1 \geq \frac{t}{4}$.

This corresponds to weak keys of the PV Knapsack.

Weak keys are identified easily: Given Ω_t, t_1 can be computed easily by detecting all the pairs of the form $(\omega, \omega^{-1}) \in \Omega_t$.

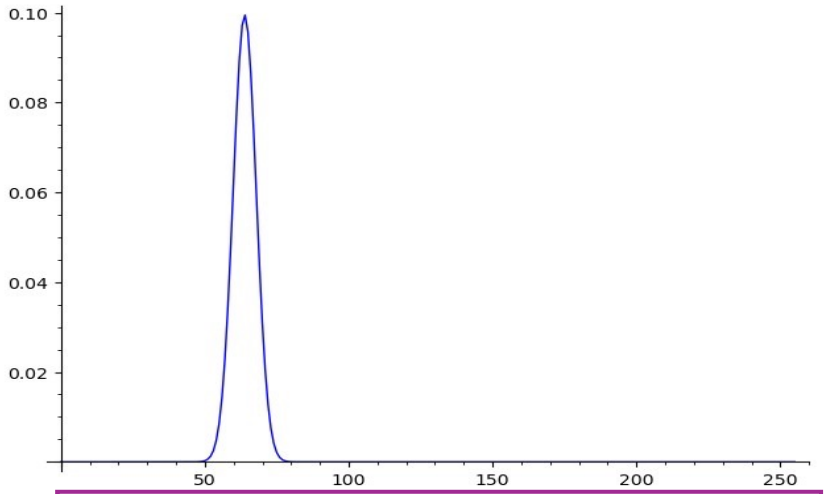
[GN'08]: N. Gama and P. Nguyen. Predicting lattice reduction. Eurocrypt'08.

The distribution of pairs for uniform Ω_t

Probability distribution of exactly t_1 pairs:

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

When $t = \frac{n}{2}$, expectation of t_1 is $\frac{t}{4}$.



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

- If the cryptosystem is used by many users, each one with its own set Ω_t , some of them will pick weak keys vulnerable to our attack.

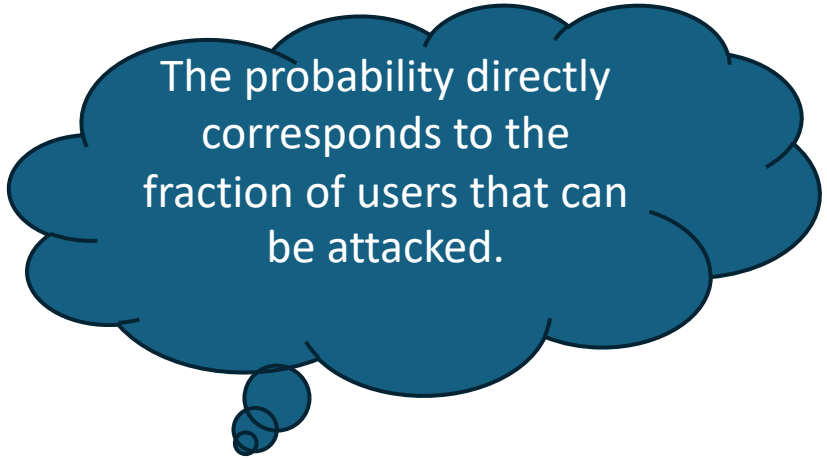
Effect of the attack on the concrete parameters

All the parameters from the literature contain a non-negligible fraction of weak keys.

Example: Practical weak key recovery of a parameter set from [HPSSW'14] with $n = 577, t = 280, q = 743177$.

The direct primal attack provides 52-bits security using the LWE estimator [APS'15].

t_1	Prob	Running time in hours	Bits operation
82	2^{-11}	115	2^{50}
84	2^{-13}	54	2^{49}
86	2^{-16}	51	2^{48}
88	2^{-19}	17	2^{46}
90	2^{-23}	6	2^{45}



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

Effect of the attack on the concrete parameters

Example: Practical weak key recovery of a parameter set from [LZA'18] with $n = 512, t = 256, q = 2^{16} + 1$.

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

t_1	Prob	Running time in hours	Bits operation
80	2^{-15}	117	2^{50}
83	2^{-19}	30	2^{48}
85	2^{-23}	9.5	2^{46}
88	2^{-30}	8	2^{45}
90	2^{-34}	7.5	2^{45}

It was initially claimed to have a 129-bit security against key recovery attack in [LZA'18], which was reduced to 87-bit security using the distinguishing attack in [BGP'22].

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

Higher order symmetry

We can also aim for higher order symmetries to reduce the lattice dimension further.

- Example: Prime n of the form $n - 1 = 0 \; mod \; 3$ [HPSSW'14], we can also use the symmetry of order 3.

But, for random Ω_t, the number of triples in $\Omega_{3t_2} = \{\omega \in \Omega_t : (\omega, \omega^\theta, \omega^{\theta^2}) \in \Omega_t\} \subseteq \Omega_t$ are reduced too much on the average!

- Probability distribution of exactly t_2 triples

$$\pi_2(t_2) = \frac{\binom{\lfloor \frac{n}{3} \rfloor}{t_2} \sum_{i=0}^{s} \binom{\lfloor \frac{n}{3} \rfloor - t_2}{i} \binom{\lfloor \frac{n}{3} \rfloor - t_2 - i}{t - 3t_2 - 2i} 3^{t-3t_2-i}}{\binom{3\lfloor \frac{n}{3} \rfloor}{t}}, s = \min\left\{\left\lfloor \frac{t - 3t_2}{2} \right\rfloor, \lfloor \frac{n}{3} \rfloor - t_2\right\}$$

Symmetry of order 2 vs 3: Practical weak key recovery from [HPSSW'14] with $n = 577, t = 280, q = 743177$.

Prob	t_1	Running time in hours	t_2	Running time in hours
2^{-26}	92	6	42	111

Thank you ☺

Paper details: eprint.iacr.org/2024/366