Partial Vandermonde Problems and PASS Encrypt

Katharina Boudgoust[1] Amin Sakzad[2] Ron Steinfeld[2]

[1]Aarhus University, Denmark

[2]Faculty of Information Technology, Monash University, Australia

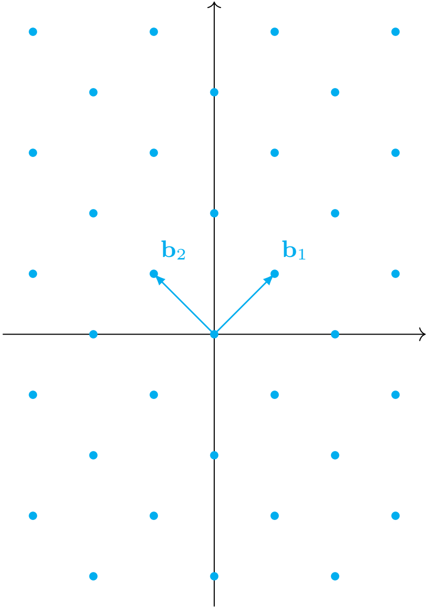
Journées C2, 11th April 2022

Lattice-Based Cryptography

Provably secure public-key cryptography needs well-defined assumptions in the form of mathematical problems.

(Main) Lattice Problems for Crypto:

- Short Integer Solution [Ajt96]
- NTRU [HPS98]
- Learning With Errors [Reg05]



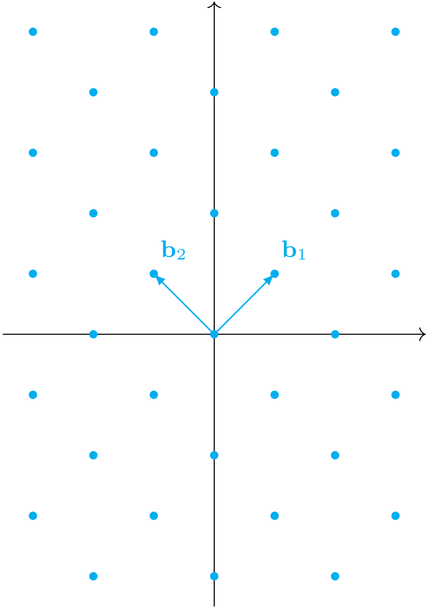
Lattice-Based Cryptography

Provably secure public-key cryptography needs well-defined assumptions in the form of mathematical problems.

(Main) Lattice Problems for Crypto:

- Short Integer Solution [Ajt96]
- NTRU [HPS98]
- Learning With Errors [Reg05]
- Partial Vandermonde Problems [HPS$^+$14]

today



Partial Vandermonde Problems

Partial Vandermonde Transform [HPS+14, LZA18]

Let $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$, with n a power-of-two ($2n$-th cyclotomic ring)

Partial Vandermonde Transform [HPS+14, LZA18]

Let $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$, with n a power-of-two ($2n$-th cyclotomic ring)

Choose q prime such that $q = 1 \bmod 2n$, then:

- it exists $2n$-th root of unity $\omega \in \mathbb{Z}_q$
- $x^n + 1 = \prod_{j \in \mathbb{Z}_{2n}^{\times}} (x - \omega^j)$

Partial Vandermonde Transform [HPS+14, LZA18]

Let $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$, with n a power-of-two ($2n$-th cyclotomic ring)

Choose q prime such that $q = 1 \bmod 2n$, then:

- it exists $2n$-th root of unity $\omega \in \mathbb{Z}_q$
- $x^n + 1 = \prod_{j \in \mathbb{Z}_{2n}^\times} (x - \omega^j)$

Write $\{\omega_j\}_{j=1,\ldots,n}$ for $\{\omega^k : k \in \mathbb{Z}_{2n}^\times\}$. This defines the **Vandermonde transform** $\mathbf{V} \colon R \to \mathbb{Z}_q^n$

$$\mathbf{V} \cdot a = \begin{bmatrix} 1 & \omega_1 & \cdots & \omega_1^{n-1} \\ 1 & \omega_2 & \cdots & \omega_2^{n-1} \\ 1 & \omega_3 & \cdots & \omega_3^{n-1} \\ \vdots & & & \vdots \\ 1 & \omega_n & \cdots & \omega_n^{n-1} \end{bmatrix} \cdot \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_n \end{bmatrix} = b \bmod q.$$

Partial Vandermonde Transform [HPS$^+$14, LZA18]

Let $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$, with n a power-of-two ($2n$-th cyclotomic ring)

Choose q prime such that $q = 1 \bmod 2n$, then:

- it exists $2n$-th root of unity $\omega \in \mathbb{Z}_q$
- $x^n + 1 = \prod_{j \in \mathbb{Z}_{2n}^\times} (x - \omega^j)$

Write $\{\omega_j\}_{j=1,\ldots,n}$ for $\{\omega^k \colon k \in \mathbb{Z}_{2n}^\times\}$. This defines the **Vandermonde transform** $\mathbf{V} \colon R \to \mathbb{Z}_q^n$

$$\mathbf{V} \cdot a = \begin{bmatrix} 1 & \omega_1 & \cdots & \omega_1^{n-1} \\ 1 & \omega_2 & \cdots & \omega_2^{n-1} \\ 1 & \omega_3 & \cdots & \omega_3^{n-1} \\ \vdots & & & \vdots \\ 1 & \omega_n & \cdots & \omega_n^{n-1} \end{bmatrix} \cdot \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_n \end{bmatrix} = b \bmod q.$$

Observation: b uniquely defines $a \bmod q$ and vice versa. ($\mathbf{V}^{-1}$ exists)

Partial Vandermonde Transform [HPS+14, LZA18]

Let $R = \mathbb{Z}[x]/\langle x^n + 1 \rangle$, with n a power-of-two ($2n$-th cyclotomic ring)

Choose q prime such that $q = 1 \bmod 2n$, then:

- it exists $2n$-th root of unity $\omega \in \mathbb{Z}_q$
- $x^n + 1 = \prod_{j \in \mathbb{Z}_{2n}^\times} (x - \omega^j)$

Write $\{\omega_j\}_{j=1,\dots,n}$ for $\{\omega^k : k \in \mathbb{Z}_{2n}^\times\}$. This defines the **Vandermonde transform** $\mathbf{V} \colon R \to \mathbb{Z}_q^n$

$$\mathbf{V} \cdot a = \begin{bmatrix} 1 & \omega_1 & \cdots & \omega_1^{n-1} \\ 1 & \omega_2 & \cdots & \omega_2^{n-1} \\ 1 & \omega_3 & \cdots & \omega_3^{n-1} \\ \vdots & & & \vdots \\ 1 & \omega_n & \cdots & \omega_n^{n-1} \end{bmatrix} \cdot \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_n \end{bmatrix} = b \bmod q.$$

Observation: b uniquely defines $a \bmod q$ and vice versa. ($\mathbf{V}^{-1}$ exists)

Question: What happens if we only provide t out of n coefficients? (say half)

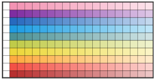
Partial Vandermonde Transform [HPS+14, LZA18]

Let $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$, with n a power-of-two ($2n$-th cyclotomic ring)

Choose q prime such that $q = 1 \bmod 2n$, then:

- it exists $2n$-th root of unity $\omega \in \mathbb{Z}_q$
- $x^n + 1 = \prod_{j \in \mathbb{Z}_{2n}^\times} (x - \omega^j)$

Write $\{\omega_j\}_{j=1,\dots,n}$ for $\{\omega^k : k \in \mathbb{Z}_{2n}^\times\}$. This defines the **Vandermonde transform** $\mathbf{V} \colon R \to \mathbb{Z}_q^n$



$$\mathbf{V} \cdot a = \begin{bmatrix} 1 & \omega_1 & \cdots & \omega_1^{n-1} \\ 1 & \omega_2 & \cdots & \omega_2^{n-1} \\ 1 & \omega_3 & \cdots & \omega_3^{n-1} \\ \vdots & & & \vdots \\ 1 & \omega_n & \cdots & \omega_n^{n-1} \end{bmatrix} \cdot \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_n \end{bmatrix} = b \bmod q.$$

Observation: b uniquely defines $a \bmod q$ and vice versa. ($\mathbf{V}^{-1}$ exists)

Question: What happens if we only provide t out of n coefficients? (say half)

Note: For $\Omega \subseteq \{\omega_j\}_{j=1,\dots,n}$ write $\mathbf{V}_\Omega \cdot a = b$. **(partial Vandermonde transform)**

Partial Vandermonde Problems

Choose a random subset $\Omega \subseteq \{\omega_j\}_{j=1,\ldots,n}$ of size $|\Omega| = t$.

Partial Vandermonde knapsack problem (PV-Knap): Sample $\mathsf{e} \sim$ DistrE over $\mathbb{Z}^n$ defining

$$\mathbf{V}_\Omega \, e = b \mod q.$$

Search: find e

Partial Vandermonde Problems

Choose a random subset $\Omega \subseteq \{\omega_j\}_{j=1,\ldots,n}$ of size $|\Omega| = t$.

Partial Vandermonde knapsack problem (PV-Knap): Sample e $\sim$ DistrE over $\mathbb{Z}^n$ defining

$$\mathbf{V}_\Omega \, e = b \mod q.$$

Search: find e

Partial Vandermonde Learning With Errors (PV-LWE): Sample s $\sim$ DistrS over $\mathbb{Z}^t$ and e $\sim$ DistrE over $\mathbb{Z}^n$ defining

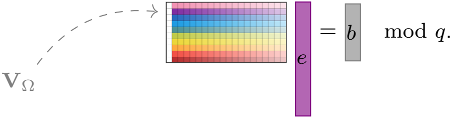
$$\mathbf{V}_\Omega^T \, s + e = b \mod q.$$

Search: find e (and secret s)

Partial Vandermonde Problems

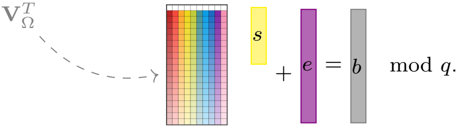
Choose a random subset $\Omega \subseteq \{\omega_j\}_{j=1,\ldots,n}$ of size $|\Omega| = t$.

Partial Vandermonde knapsack problem (PV-Knap): Sample e $\sim$ DistrE over $\mathbb{Z}^n$ defining



Search: find e

Partial Vandermonde Learning With Errors (PV-LWE): Sample s $\sim$ DistrS over $\mathbb{Z}^t$ and e $\sim$ DistrE over $\mathbb{Z}^n$ defining



Search: find e (and secret s)

Conjecture: Hard to solve if DistrE provides elements of small norm.

Equivalence of PV-Knap and PV-LWE

Let $t = n/2$ and set $\mathcal{P}_t = \{\Omega \subseteq \{\omega_j\}_{j=1,\dots,n} \colon |\Omega| = t\}$.

Property 1: $\mathbf{V}_\Omega$ defines a ring homomorphism from R to $\mathbb{Z}_q^t$:

$$\mathbf{V}_\Omega(a \cdot b) = (\mathbf{V}_\Omega a) \circ (\mathbf{V}_\Omega b)$$

(component-wise multiplication $\circ$)

Equivalence of PV-Knap and PV-LWE

Let $t = n/2$ and set $\mathcal{P}_t = \{\Omega \subseteq \{\omega_j\}_{j=1,\ldots,n} \colon |\Omega| = t\}$.

Property 1: $\mathbf{V}_\Omega$ defines a ring homomorphism from R to $\mathbb{Z}_q^t$:

$$\mathbf{V}_\Omega(a \cdot b) = (\mathbf{V}_\Omega a) \circ (\mathbf{V}_\Omega b)$$

(component-wise multiplication $\circ$)

Property 2: $\Omega^c = \{\omega_j\}_j \setminus \Omega$ defines the **complement** partial Vandermonde transform $\mathbf{V}_{\Omega^c}$.
Given $\mathbf{V}_\Omega a$ and $\mathbf{V}_{\Omega^c} a$, we can recover $a \bmod q$.

Equivalence of PV-Knap and PV-LWE

Let $t = n/2$ and set $\mathcal{P}_t = \{\Omega \subseteq \{\omega_j\}_{j=1,\dots,n} \colon |\Omega| = t\}$.

Property 1: $\mathbf{V}_\Omega$ defines a ring homomorphism from R to $\mathbb{Z}_q^t$:

$$\mathbf{V}_\Omega(a \cdot b) = (\mathbf{V}_\Omega a) \circ (\mathbf{V}_\Omega b)$$

(component-wise multiplication $\circ$)

Property 2: $\Omega^c = \{\omega_j\}_j \setminus \Omega$ defines the **complement** partial Vandermonde transform $\mathbf{V}_{\Omega^c}$.
Given $\mathbf{V}_\Omega a$ and $\mathbf{V}_{\Omega^c} a$, we can recover $a \bmod q$.

Property 3: For every $\Omega \in \mathcal{P}_t$, there exists a $\Omega' \in \mathcal{P}_t$ such that

$$\mathbf{V}_{\Omega'} \cdot \mathbf{V}_\Omega^T = 0 \in \mathbb{Z}_q^{t \times t}.$$

(parity check matrix, ⚠ only for power-of-two cyclotomics)

Equivalence of PV-Knap and PV-LWE

Let $t = n/2$ and set $\mathcal{P}_t = \{\Omega \subseteq \{\omega_j\}_{j=1,\ldots,n} \colon |\Omega| = t\}$.

Property 1: $\mathbf{V}_\Omega$ defines a ring homomorphism from R to $\mathbb{Z}_q^t$:

$$\mathbf{V}_\Omega(a \cdot b) = (\mathbf{V}_\Omega a) \circ (\mathbf{V}_\Omega b)$$

(component-wise multiplication $\circ$)

Property 2: $\Omega^c = \{\omega_j\}_j \setminus \Omega$ defines the **complement** partial Vandermonde transform $\mathbf{V}_{\Omega^c}$. Given $\mathbf{V}_\Omega a$ and $\mathbf{V}_{\Omega^c} a$, we can recover $a \bmod q$.

Property 3: For every $\Omega \in \mathcal{P}_t$, there exists a $\Omega' \in \mathcal{P}_t$ such that

$$\mathbf{V}_{\Omega'} \cdot \mathbf{V}_\Omega^T = 0 \in \mathbb{Z}_q^{t \times t}.$$

(parity check matrix, ⚠ only for power-of-two cyclotomics)

Lemma (Adapted [MM11, Sec. 4.2])

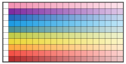
Let ψ denote a distribution over $\mathbb{Z}^n \cong R$. There is an efficient reduction from PV-LWE$_\psi$ to PV-Knap$_\psi$, and vice versa.

Idea: Given $(\mathbf{V}_\Omega, b)$, with $b = \mathbf{V}_\Omega^T s + e$. Compute Ω' such that $\mathbf{V}_{\Omega'} \cdot \mathbf{V}_\Omega^T = 0$.
Then, $b' := \mathbf{V}_{\Omega'} b = \mathbf{V}_{\Omega'} e$ is an instance of PV-Knap.

Hidden Ideal Lattice 1/2

Choose a random subset $\Omega \subseteq \{\omega_j\}_{j=1,\dots,n}$ of size $|\Omega| = t$.

Partial Vandermonde knapsack problem (PV-Knap): Sample e $\sim$ DistrE over $\mathbb{Z}^n$ defining



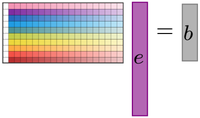
$$e = b \mod q.$$

Search: find e

Hidden Ideal Lattice 1/2

Choose a random subset $\Omega \subseteq \{\omega_j\}_{j=1,\ldots,n}$ of size $|\Omega| = t$.

Partial Vandermonde knapsack problem (PV-Knap): Sample e $\sim$ DistrE over $\mathbb{Z}^n$ defining



$$\mod q.$$

Search: find e

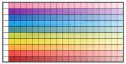
The matrix $\mathbf{V}_\Omega$ defines an **ideal lattice**:

$$\Lambda_q^{\perp}(\mathbf{V}_\Omega) = \{a \in R \colon \mathbf{V}_\Omega a = 0 \bmod q\}$$

Hidden Ideal Lattice 1/2

Choose a random subset $\Omega \subseteq \{\omega_j\}_{j=1,\dots,n}$ of size $|\Omega| = t$.

Partial Vandermonde knapsack problem (PV-Knap): Sample e $\sim$ DistrE over $\mathbb{Z}^n$ defining



$$e = b \mod q.$$

Search: find e

The matrix $\mathbf{V}_\Omega$ defines an **ideal lattice**:

$$\Lambda_q^\perp(\mathbf{V}_\Omega) = \{a \in R \colon \mathbf{V}_\Omega a = 0 \bmod q\}$$

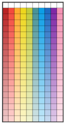
Idea:

1) Solve $\mathbf{V}_\Omega y = b \bmod q$ for the unknown y in R (in general not in the support of DistrE)
2) Find a **closet vector** v of y in $\Lambda_q^\perp(\mathbf{V}_\Omega)$, i.e., $\|y - v\|$ smallest
3) The element $e := y - v$ is a solution to PV-Knap

⚠ Promise variant of the closest vector problem, called **Bounded Distance Decoding (BDD)**

Hidden Ideal Lattice 2/2

Partial Vandermonde Learning With Errors (PV-LWE): Sample s $\sim$ DistrS over $\mathbb{Z}^t$ and e $\sim$ DistrE over $\mathbb{Z}^n$ defining

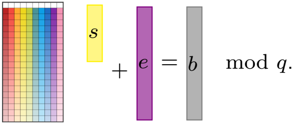


$$s + e = b \mod q.$$

Search: find e (and secret s)

Hidden Ideal Lattice 2/2

Partial Vandermonde Learning With Errors (PV-LWE): Sample s $\sim$ DistrS over $\mathbb{Z}^t$ and e $\sim$ DistrE over $\mathbb{Z}^n$ defining



Search: find e (and secret s)

This is an instance of **BDD** in the **ideal lattice**

$$\Lambda_q(\mathbf{V}_\Omega) = \{a \in R \colon a = \mathbf{V}_\Omega^T s \bmod q \text{ for some } s \in \mathbb{Z}_q^t\}$$

PASS Encrypt

PASS Encrypt [HS15]

[HS15]	Our work
deterministic	randomized
without proof of security	with proof of security
fixed $\mathbf{V}_\Omega$	random $\mathbf{V}_\Omega$

PASS Encrypt [HS15]

[HS15]	Our work
deterministic	randomized
without proof of security	with proof of security
fixed $\mathbf{V}_\Omega$	random $\mathbf{V}_\Omega$

Let $p \ll q$ be two primes, $m \in \{0,1\}^n$, ψ a distribution over $\mathbb{Z}^n$ and $t = n/2$.

KeyGen(1^λ): sample $f \leftarrow \psi$ and $\Omega \leftarrow \mathsf{Unif}(\mathcal{P}_t)$; return $\mathsf{sk} = f$ and $\mathsf{pk} = (\Omega, \mathbf{V}_\Omega f)$

Enc(pk, m): sample $r, s \leftarrow \psi$; set $r' = pr$ and $s' = m + ps$

$$e_1 = (\mathsf{pk} \circ \mathbf{V}_\Omega r') + \mathbf{V}_\Omega s'$$
$$e_2 = \mathbf{V}_{\Omega^c} r'$$
$$e_3 = \mathbf{V}_{\Omega^c} s'$$

return $c = (e_1, e_2, e_3)$

Dec(sk, c): compute $c' = (\mathbf{V}_{\Omega^c} \mathsf{sk} \circ e_2) + e_3$ and combine with e_1 to $c'' \in \mathbb{Z}_q^n$;
return $\mathbf{V}^{-1} c'' \bmod p$.

PASS Encrypt [HS15]

[HS15]	Our work
deterministic	randomized
without proof of security	with proof of security
fixed $\mathbf{V}_\Omega$	random $\mathbf{V}_\Omega$

Let $p \ll q$ be two primes, $m \in \{0,1\}^n$, ψ a distribution over $\mathbb{Z}^n$ and $t = n/2$.

KeyGen(1^λ): sample $f \leftarrow \psi$ and $\Omega \leftarrow \mathsf{Unif}(\mathcal{P}_t)$; return $\mathsf{sk} = f$ and $\mathsf{pk} = (\Omega, \mathbf{V}_\Omega f)$

Enc(pk, m): sample $r, s \leftarrow \psi$; set $r' = pr$ and $s' = m + ps$

$$e_1 = (\mathsf{pk} \circ \mathbf{V}_\Omega r') + \mathbf{V}_\Omega s'$$
$$e_2 = \mathbf{V}_{\Omega^c} r'$$
$$e_3 = \mathbf{V}_{\Omega^c} s'$$

return $c = (e_1, e_2, e_3)$

Dec(sk, c): compute $c' = (\mathbf{V}_{\Omega^c} \mathsf{sk} \circ e_2) + e_3$ and combine with e_1 to $c'' \in \mathbb{Z}_q^n$; return $\mathbf{V}^{-1} c'' \bmod p$.

PASS Encrypt [HS15]

[HS15]	Our work
deterministic	randomized
without proof of security	with proof of security
fixed $\mathbf{V}_\Omega$	random $\mathbf{V}_\Omega$

Let $p \ll q$ be two primes, $m \in \{0,1\}^n$, ψ a distribution over $\mathbb{Z}^n$ and $t = n/2$.

KeyGen(1^λ): sample $f \leftarrow \psi$ and $\Omega \leftarrow \mathsf{Unif}(\mathcal{P}_t)$; return $\mathsf{sk} = f$ and $\mathsf{pk} = (\Omega, \mathbf{V}_\Omega f)$

Enc(pk, m): sample $r, s \leftarrow \psi$; set $r' = pr$ and $s' = m + ps$

$$e_1 = (\mathsf{pk} \circ \mathbf{V}_\Omega r') + \mathbf{V}_\Omega s'$$
$$e_2 = \mathbf{V}_{\Omega^c} r'$$
$$e_3 = \mathbf{V}_{\Omega^c} s'$$

return $c = (e_1, e_2, e_3)$

Dec(sk, c): compute $c' = (\mathbf{V}_{\Omega^c} \mathsf{sk} \circ e_2) + e_3$ and combine with e_1 to $c'' \in \mathbb{Z}_q^n$; return $\mathbf{V}^{-1} c'' \bmod p$.

PASS Encrypt [HS15]

[HS15]	Our work
deterministic	randomized
without proof of security	with proof of security
fixed $\mathbf{V}_\Omega$	random $\mathbf{V}_\Omega$

Let $p \ll q$ be two primes, $m \in \{0,1\}^n$, ψ a distribution over $\mathbb{Z}^n$ and $t = n/2$.

KeyGen(1^λ): sample $f \leftarrow \psi$ and $\Omega \leftarrow \mathsf{Unif}(\mathcal{P}_t)$; return $\mathsf{sk} = f$ and $\mathsf{pk} = (\Omega, \mathbf{V}_\Omega f)$

Enc(pk, m): sample $r, s \leftarrow \psi$; set $r' = pr$ and $s' = m + ps$

$$e_1 = (\mathsf{pk} \circ \mathbf{V}_\Omega r') + \mathbf{V}_\Omega s'$$
$$e_2 = \mathbf{V}_{\Omega^c} r'$$
$$e_3 = \mathbf{V}_{\Omega^c} s'$$

return $c = (e_1, e_2, e_3)$

Dec(sk, c): compute $c' = (\mathbf{V}_{\Omega^c} \mathsf{sk} \circ e_2) + e_3$ and combine with e_1 to $c'' \in \mathbb{Z}_q^n$;
return $\mathbf{V}^{-1} c'' \bmod p$.

Recall: $\mathbf{V}_\Omega$ and $\mathbf{V}_{\Omega^c}$ define $\mathbf{V}$ and $\mathbf{V}^{-1}$.

PASS Encrypt [HS15]

[HS15]	Our work
deterministic	randomized
without proof of security	with proof of security
fixed $\mathbf{V}_\Omega$	random $\mathbf{V}_\Omega$

Let $p \ll q$ be two primes, $m \in \{0,1\}^n$, ψ a distribution over $\mathbb{Z}^n$ and $t = n/2$.

KeyGen(1^λ): sample $f \leftarrow \psi$ and $\Omega \leftarrow \mathsf{Unif}(\mathcal{P}_t)$; return $\mathsf{sk} = f$ and $\mathsf{pk} = (\Omega, \mathbf{V}_\Omega f)$

Enc(pk, m): sample $r, s \leftarrow \psi$; set $r' = pr$ and $s' = m + ps$

$$e_1 = (\mathsf{pk} \circ \mathbf{V}_\Omega r') + \mathbf{V}_\Omega s'$$
$$e_2 = \mathbf{V}_{\Omega^c} r'$$
$$e_3 = \mathbf{V}_{\Omega^c} s'$$

return $c = (e_1, e_2, e_3)$

Dec(sk, c): compute $c' = (\mathbf{V}_{\Omega^c}\mathsf{sk} \circ e_2) + e_3$ and combine with e_1 to $c'' \in \mathbb{Z}_q^n$;
return $\mathbf{V}^{-1} c'' \bmod p$.

Recall: $\mathbf{V}_\Omega$ and $\mathbf{V}_{\Omega^c}$ define $\mathbf{V}$ and $\mathbf{V}^{-1}$.

Correctness:

$$\left.\begin{aligned} e_1 &= (\mathbf{V}_\Omega f \circ \mathbf{V}_\Omega r') + \mathbf{V}_\Omega s' = \mathbf{V}_\Omega (f \cdot r' + s') \\ c' &= (\mathbf{V}_{\Omega^c}\mathsf{sk} \circ (\mathbf{V}_{\Omega^c} r') + \mathbf{V}_{\Omega^c} s' = \mathbf{V}_{\Omega^c}(f \cdot r' + s') \end{aligned}\right\} \text{ring homomorphism}$$

PASS Encrypt [HS15]

[HS15]	Our work
deterministic	randomized
without proof of security	with proof of security
fixed $\mathbf{V}_\Omega$	random $\mathbf{V}_\Omega$

Let $p \ll q$ be two primes, $m \in \{0,1\}^n$, ψ a distribution over $\mathbb{Z}^n$ and $t = n/2$.

KeyGen(1^λ): sample $f \leftarrow \psi$ and $\Omega \leftarrow \mathsf{Unif}(\mathcal{P}_t)$; return $\mathsf{sk} = f$ and $\mathsf{pk} = (\Omega, \mathbf{V}_\Omega f)$

Enc(pk, m): sample $r, s \leftarrow \psi$; set $r' = pr$ and $s' = m + ps$

$$e_1 = (\mathsf{pk} \circ \mathbf{V}_\Omega r') + \mathbf{V}_\Omega s'$$
$$e_2 = \mathbf{V}_{\Omega^c} r'$$
$$e_3 = \mathbf{V}_{\Omega^c} s'$$

return $c = (e_1, e_2, e_3)$

Dec(sk, c): compute $c' = (\mathbf{V}_{\Omega^c} \mathsf{sk} \circ e_2) + e_3$ and combine with e_1 to $c'' \in \mathbb{Z}_q^n$;
return $\mathbf{V}^{-1} c'' \bmod p$.

Recall: $\mathbf{V}_\Omega$ and $\mathbf{V}_{\Omega^c}$ define $\mathbf{V}$ and $\mathbf{V}^{-1}$.

Correctness:

$$\left.\begin{aligned} e_1 &= (\mathbf{V}_\Omega f \circ \mathbf{V}_\Omega r') + \mathbf{V}_\Omega s' = \mathbf{V}_\Omega (f \cdot r' + s') \\ c' &= (\mathbf{V}_{\Omega^c} \mathsf{sk} \circ (\mathbf{V}_{\Omega^c} r') + \mathbf{V}_{\Omega^c} s' = \mathbf{V}_{\Omega^c} (f \cdot r' + s') \end{aligned}\right\} \text{ring homomorphism}$$

$$\mathbf{V}^{-1}(e_1 || c') = \mathbf{V}^{-1}(\mathbf{V}(f \cdot r' + s')) = f \cdot pr + ps + m = m \bmod p$$

if f, r and s are small enough

PASS Encrypt [HS15]

[HS15]	Our work
deterministic	randomized
without proof of security	with proof of security
fixed $\mathbf{V}_\Omega$	random $\mathbf{V}_\Omega$

Let $p \ll q$ be two primes, $m \in \{0,1\}^n$, ψ a distribution over $\mathbb{Z}^n$ and $t = n/2$.

KeyGen(1^λ): sample $f \leftarrow \psi$ and $\Omega \leftarrow \mathsf{Unif}(\mathcal{P}_t)$; return $\mathsf{sk} = f$ and $\mathsf{pk} = (\Omega, \mathbf{V}_\Omega f)$

Enc(pk, m): sample $r, s \leftarrow \psi$; set $r' = pr$ and $s' = m + ps$

$$e_1 = (\mathsf{pk} \circ \mathbf{V}_\Omega r') + \mathbf{V}_\Omega s'$$
$$e_2 = \mathbf{V}_{\Omega^c} r'$$
$$e_3 = \mathbf{V}_{\Omega^c} s'$$

return $c = (e_1, e_2, e_3)$

Dec(sk, c): compute $c' = (\mathbf{V}_{\Omega^c} \mathsf{sk} \circ e_2) + e_3$ and combine with e_1 to $c'' \in \mathbb{Z}_q^n$; return $\mathbf{V}^{-1} c'' \bmod p$.

PASS Encrypt [HS15]

[HS15]	Our work
deterministic	randomized
without proof of security	with proof of security
fixed $\mathbf{V}_\Omega$	random $\mathbf{V}_\Omega$

Let $p \ll q$ be two primes, $m \in \{0,1\}^n$, ψ a distribution over $\mathbb{Z}^n$ and $t = n/2$.

KeyGen(1^λ): sample $f \leftarrow \psi$ and $\Omega \leftarrow \mathsf{Unif}(\mathcal{P}_t)$; return $\mathsf{sk} = f$ and $\mathsf{pk} = (\Omega, \mathbf{V}_\Omega f)$

Enc(pk, m): sample $r, s \leftarrow \psi$; set $r' = pr$ and $s' = m + ps$

$$e_1 = (\mathsf{pk} \circ \mathbf{V}_\Omega r') + \mathbf{V}_\Omega s' = \mathbf{V}_\Omega (f \cdot r' + s')$$
$$e_2 = \mathbf{V}_{\Omega^c} r'$$
$$e_3 = \mathbf{V}_{\Omega^c} s'$$

return $c = (e_1, e_2, e_3)$

Dec(sk, c): compute $c' = (\mathbf{V}_{\Omega^c} \mathsf{sk} \circ e_2) + e_3$ and combine with e_1 to $c'' \in \mathbb{Z}_q^n$; return $\mathbf{V}^{-1} c'' \bmod p$.

Security:
$e_1 = \mathbf{V}_\Omega (f \cdot r' + s')$ defines an instance of PV-Knap

PASS Encrypt [HS15]

[HS15]	Our work
deterministic	randomized
without proof of security	with proof of security
fixed $\mathbf{V}_\Omega$	random $\mathbf{V}_\Omega$

Let $p \ll q$ be two primes, $m \in \{0,1\}^n$, ψ a distribution over $\mathbb{Z}^n$ and $t = n/2$.

KeyGen(1^λ): sample $f \leftarrow \psi$ and $\Omega \leftarrow \mathsf{Unif}(\mathcal{P}_t)$; return $\mathsf{sk} = f$ and $\mathsf{pk} = (\Omega, \mathbf{V}_\Omega f)$

Enc(pk, m): sample $r, s \leftarrow \psi$; set $r' = pr$ and $s' = m + ps$

$$e_1 = (\mathsf{pk} \circ \mathbf{V}_\Omega r') + \mathbf{V}_\Omega s' = \mathbf{V}_\Omega(f \cdot r' + s')$$
$$e_2 = \mathbf{V}_{\Omega^c} r'$$
$$e_3 = \mathbf{V}_{\Omega^c} s'$$

return $c = (e_1, e_2, e_3)$

Dec(sk, c): compute $c' = (\mathbf{V}_{\Omega^c}\mathsf{sk} \circ e_2) + e_3$ and combine with e_1 to $c'' \in \mathbb{Z}_q^n$; return $\mathbf{V}^{-1}c'' \bmod p$.

Security:
$e_1 = \mathbf{V}_\Omega(f \cdot r' + s')$ defines an instance of PV-Knap with pk, e_2 and e_3 as additional information.

$\Rightarrow$ leaky variant of **PV-Knap**, that we call the **PASS problem**.

PASS Encrypt [HS15]

[HS15]	Our work
deterministic	randomized
without proof of security	with proof of security
fixed $\mathbf{V}_\Omega$	random $\mathbf{V}_\Omega$

Let $p \ll q$ be two primes, $m \in \{0,1\}^n$, ψ a distribution over $\mathbb{Z}^n$ and $t = n/2$.

KeyGen(1^λ): sample $f \leftarrow \psi$ and $\Omega \leftarrow \mathsf{Unif}(\mathcal{P}_t)$; return $\mathsf{sk} = f$ and $\mathsf{pk} = (\Omega, \mathbf{V}_\Omega f)$

Enc(pk, m): sample $r, s \leftarrow \psi$; set $r' = pr$ and $s' = m + ps$

$$e_1 = (\mathsf{pk} \circ \mathbf{V}_\Omega r') + \mathbf{V}_\Omega s' = \mathbf{V}_\Omega (f \cdot r' + s')$$
$$e_2 = \mathbf{V}_{\Omega^c} r'$$
$$e_3 = \mathbf{V}_{\Omega^c} s'$$

return $c = (e_1, e_2, e_3)$

Dec(sk, c): compute $c' = (\mathbf{V}_{\Omega^c} \mathsf{sk} \circ e_2) + e_3$ and combine with e_1 to $c'' \in \mathbb{Z}_q^n$; return $\mathbf{V}^{-1} c'' \bmod p$.

Security:
$e_1 = \mathbf{V}_\Omega (f \cdot r' + s')$ defines an instance of PV-Knap with pk, e_2 and e_3 as additional information.

$\Rightarrow$ leaky variant of **PV-Knap**, that we call the **PASS problem**.

⚠ PASS problem is tailored to PASS Encrypt!
? Reduce it from some more general problem?

Properties of PASS Encrypt

Homomorphic properties:

Addition: $\mathsf{Enc}(\mathsf{pk}, m_1) + \mathsf{Enc}(\mathsf{pk}, m_2) = \mathsf{Enc}(\mathsf{pk}, m_1 + m_2)$

Multiplication: $\mathsf{Enc}(\mathsf{pk}, m_1) \circ \mathsf{Enc}(\mathsf{pk}, m_2) = \mathsf{Enc}(\mathsf{pk}, m_1 \cdot m_2)$

Properties of PASS Encrypt

Homomorphic properties:

Addition: $\mathsf{Enc}(\mathsf{pk}, m_1) + \mathsf{Enc}(\mathsf{pk}, m_2) = \mathsf{Enc}(\mathsf{pk}, m_1 + m_2)$

Multiplication: $\mathsf{Enc}(\mathsf{pk}, m_1) \circ \mathsf{Enc}(\mathsf{pk}, m_2) = \mathsf{Enc}(\mathsf{pk}, m_1 \cdot m_2)$

⚠ For $\circ$, need of 1 additional cross-term and the decryption algorithm has to be changed.

Properties of PASS Encrypt

Homomorphic properties:

Addition: $\mathsf{Enc}(\mathsf{pk}, m_1) + \mathsf{Enc}(\mathsf{pk}, m_2) = \mathsf{Enc}(\mathsf{pk}, m_1 + m_2)$

Multiplication: $\mathsf{Enc}(\mathsf{pk}, m_1) \circ \mathsf{Enc}(\mathsf{pk}, m_2) = \mathsf{Enc}(\mathsf{pk}, m_1 \cdot m_2)$

⚠ For $\circ$, need of 1 additional cross-term and the decryption algorithm has to be changed.

Efficiency:

Scheme	NTRU [HPS98]	P-LWE Regev [LP11]	PASS Encrypt
$\frac{\lvert c\rvert + \lvert \mathsf{pk}\rvert}{\lvert m\rvert}$	$2\log_2 q$	$3\log_2 q$	$2.5\log_2 q$

Properties of PASS Encrypt

Homomorphic properties:

Addition: $\mathsf{Enc}(\mathsf{pk}, m_1) + \mathsf{Enc}(\mathsf{pk}, m_2) = \mathsf{Enc}(\mathsf{pk}, m_1 + m_2)$

Multiplication: $\mathsf{Enc}(\mathsf{pk}, m_1) \circ \mathsf{Enc}(\mathsf{pk}, m_2) = \mathsf{Enc}(\mathsf{pk}, m_1 \cdot m_2)$

⚠ For $\circ$, need of 1 additional cross-term and the decryption algorithm has to be changed.

Efficiency:

Scheme	NTRU [HPS98]	P-LWE Regev [LP11]	PASS Encrypt
$\frac{\lvert c\rvert + \lvert \mathsf{pk}\rvert}{\lvert m\rvert}$	$2\log_2 q$	$3\log_2 q$	$2.5\log_2 q$

Properties of PASS Encrypt

Homomorphic properties:

Addition: $\mathsf{Enc}(\mathsf{pk}, m_1) + \mathsf{Enc}(\mathsf{pk}, m_2) = \mathsf{Enc}(\mathsf{pk}, m_1 + m_2)$

Multiplication: $\mathsf{Enc}(\mathsf{pk}, m_1) \circ \mathsf{Enc}(\mathsf{pk}, m_2) = \mathsf{Enc}(\mathsf{pk}, m_1 \cdot m_2)$

⚠ For $\circ$, need of 1 additional cross-term and the decryption algorithm has to be changed.

Efficiency:

Scheme	NTRU [HPS98]	P-LWE Regev [LP11]	PASS Encrypt
$\frac{\lvert c\rvert + \lvert \mathsf{pk}\rvert}{\lvert m\rvert}$	$2\log_2 q$	$3\log_2 q$	$2.5\log_2 q$

Concrete Security:

Known: key recovery and randomness recovery attacks [HS15, DHSS20]

New: plaintext recovery using hints attacks

💡 make use of leaky LWE estimator of Dachman-Soled et al. [DDGR20]

Conclusion and Perspectives

Open Questions and Perspectives

Follow-ups

- Construct encryption scheme based only on PV-LWE / PV-Knap

Questions **?**

- Hardness of partial Vandermonde problems
  - Cryptanalysis?
  - Worst-case to average-case reductions as for LWE?
- More cryptographic applications

Thank you.

Miklós Ajtai.
Generating hard instances of lattice problems (extended abstract).
In *STOC*, pages 99–108. ACM, 1996.

Dana Dachman-Soled, Léo Ducas, Huijing Gong, and Mélissa Rossi.
LWE with side information: Attacks and concrete security estimation.
In *CRYPTO (2)*, volume 12171 of *Lecture Notes in Computer Science*, pages 329–358. Springer, 2020.

Yarkin Doröz, Jeffrey Hoffstein, Joseph H. Silverman, and Berk Sunar.
MMSAT: A scheme for multimessage multiuser signature aggregation.
IACR Cryptol. ePrint Arch., page 520, 2020.

Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman.
NTRU: A ring-based public key cryptosystem.
In *ANTS*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer, 1998.

Jeffrey Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman, and William Whyte.
Practical signatures from the partial fourier recovery problem.
In *ACNS*, volume 8479 of *Lecture Notes in Computer Science*, pages 476–493. Springer, 2014.

Jeffrey Hoffstein and Joseph H. Silverman.
Pass-encrypt: a public key cryptosystem based on partial evaluation of polynomials.

Des. Codes Cryptogr., 77(2-3):541–552, 2015.

Richard Lindner and Chris Peikert.
Better key sizes (and attacks) for lwe-based encryption.
In *CT-RSA*, volume 6558 of *Lecture Notes in Computer Science*, pages 319–339. Springer, 2011.

Xingye Lu, Zhenfei Zhang, and Man Ho Au.
Practical signatures from the partial fourier recovery problem revisited: A provably-secure and gaussian-distributed construction.
In *ACISP*, volume 10946 of *Lecture Notes in Computer Science*, pages 813–820. Springer, 2018.

Daniele Micciancio and Petros Mol.
Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions.
In *CRYPTO*, volume 6841 of *Lecture Notes in Computer Science*, pages 465–484. Springer, 2011.

Oded Regev.
On lattices, learning with errors, random linear codes, and cryptography.
In *STOC*, pages 84–93. ACM, 2005.

Peter W. Shor.
Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.

SIAM J. Comput., 26(5):1484–1509, 1997.