A History of Lattice-Based Encryption
(in order of increasing efficiency)

Vadim Lyubashevsky
INRIA / ENS, Paris

Lattice-Based Encryption Schemes

1. NTRU [Hoffstein, Pipher, Silverman '98]

2. LWE-Based [Regev '05]

3. Ring-LWE Based [L, Peikert, Regev '10]

4. "NTRU-like" with a proof of security [Stehle, Steinfeld '11]

Subset Sum Problem

Subset-Sum Based [L, Palacio, Segev ‘10]

LWE-Based [Regev ‘05]

Ring-LWE Based [L, Peikert, Regev ’10]

“NTRU-like” with a proof of security [Stehle, Steinfeld ‘11]

NTRU [Hoffstein, Pipher, Silverman ‘98]

THE SUBSET SUM PROBLEM

Subset Sum Problem

a_i , T in $\mathbf{Z}_M$

a_i are chosen randomly

T is a sum of a random subset of the a_i

a_1 a_2 a_3 … a_n T

Find a subset of a_i's
that sums to T (mod M)

Subset Sum Problem

a_i , T in $\mathbf{Z}_{49}$

a_i are chosen randomly

T is a sum of a random subset of the a_i

15 31 24 3 14 11

$15 + 31 + 14 = 11 \pmod{49}$

How Hard is Subset Sum?

a_i , T in $\mathbf{Z}_M$

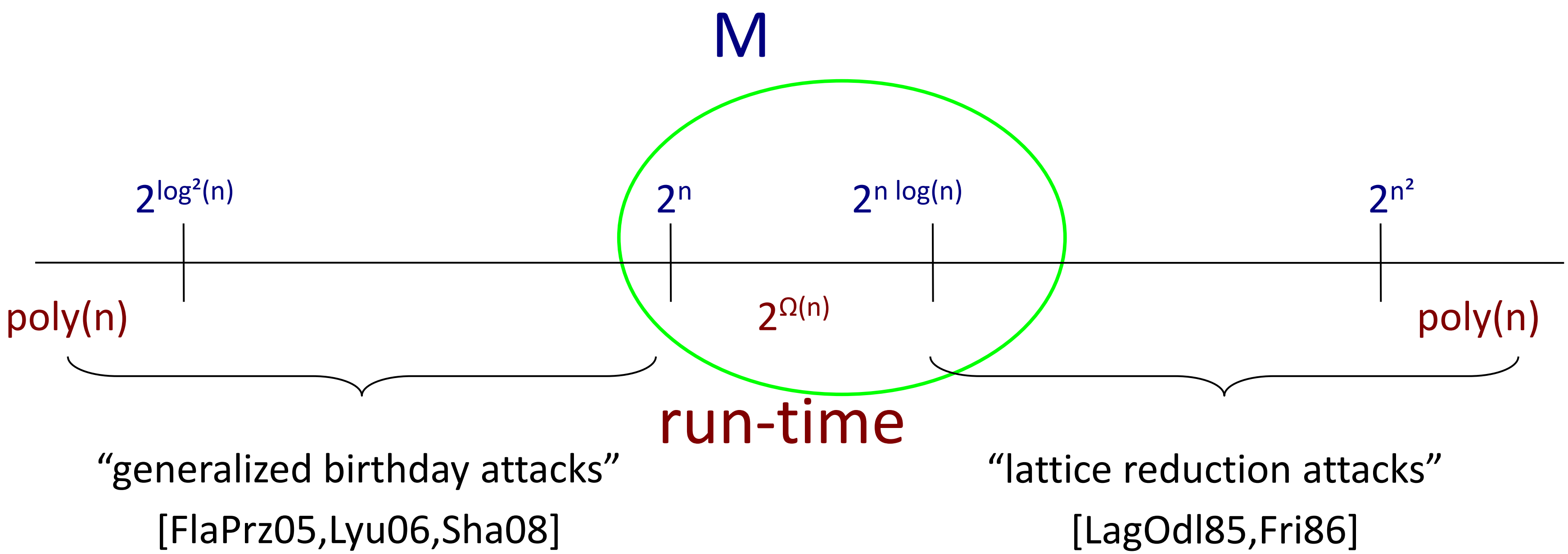
a_1 a_2 a_3 … a_n T

Find a subset of a_i's that sums to T (mod M)

<u>Hardness Depends on</u>:

- Size of n and M
- Relationship between n and M

Complexity of Solving Subset Sum



Subset Sum Crypto

- Why?
  - simple operations
  - exponential hardness
  - very different from number theoretic assumptions
  - resists quantum attacks

Subset Sum is "Pseudorandom"

[Impagliazzo-Naor 1989]:

For random $a_1,\ldots,a_n$ in Z_M and random $x_1,\ldots,x_n$ in {0,1},

distinguishing the distribution

$$(a_1,\ldots,a_n,\ a_1x_1+\ldots+a_nx_n \bmod M)$$

from the uniform distribution $U(Z_M^{n+1})$

is as hard as finding $x_1,\ldots,x_n$

What About Public-Key Encryption?

- Many early attempts
- None of them had proofs of security
- All seem to be broken

Merkle-Hellman Cryptosystem

$a_1,\ldots,a_n$ are *super-increasing* ($a_j > a_1+\ldots+a_{j-1}$)

knowing $a_1,\ldots,a_n$ and $a_1x_1+\ldots+a_nx_n$, we can recover all the x_i

Secret key: Super-increasing $a_1,\ldots,a_n$, and

$M > a_1+\ldots+a_n$ and r such that $\gcd(r,M)=1$

Public Key: $w_i=ra_i \bmod M$

$\text{Encrypt}(x_1,\ldots,x_n)=w_1x_1+\ldots+w_nx_n$

$=r(a_1x_1+\ldots+a_nx_n)$

Decrypt(T): Compute $r^{-1}T \bmod M$

and recover all x_i

Merkle-Hellman Cryptosystem

$a_1,\ldots,a_n$ are *super-increasing* $(a_j > a_1+\ldots+a_{j-1})$

knowing $a_1,\ldots,a_n$ and $a_1x_1+\ldots+a_nx_n$, we can recover all the x_i

<u>Secret key</u>: Super-increasing $a_1,\ldots,a_n$, and

$M > a_1+\ldots+a_n$ and r such that gcd(r,M)=1

<u>Public Key</u>: $w_i=ra_i \bmod M$

Encrypt($x_1,\ldots,x_n$)=$w_1x_1+\ldots+w_nx_n$

$r(a_1x_1+\ldots+a_nx_n)$

Decrypt(

Not Random!!

(was exploited in attacks)

CRYPTOSYSTEM BASED ON SUBSET SUM

[L, PALACIO, SEGEV 2010]

Subset Sum Cryptosystem

- Semantically secure based on Subset Sum for $M \approx n^n$
- Main tools

  Subset sum is pseudo-random

  Addition in $(Z_q)^n$ is "kind of like" addition in Z_M where $M=q^n$
- The proof is very simple

Facts About Addition

Want to add 4679 + 3907 + 8465 + 1343 mod 10^4

2	1	2							
4	6	7	9			4	6	7	9
3	9	0	7			3	9	0	7
8	4	6	5			8	4	6	5
1	3	4	3			1	3	4	3
8	3	9	4			6	2	7	4

Adding n numbers (written in base q) modulo q^m

→ carries < n

If q>>n, then Adding with carries ≈ Adding without carries

(i.e. in Z_M) (i.e. in $(Z_q)^n$)

So...

1 1 0 1

4 6 7 9
3 9 0 7
8 4 6 5
1 6 4 3

= 8 1 1 9

NOT Pseudorandom!

1 1 0 1

4 6 7 9
3 9 0 7
8 4 6 5
1 6 4 3

\+ 2 1 1 0

= 0 2 2 9

Pseudorandom based on Subset Sum!

Column Subset Sum Addition Is Also Pseudorandom

$$\begin{pmatrix} 4 & 6 & 7 & 9 \\ 3 & 9 & 0 & 7 \\ 8 & 4 & 6 & 5 \\ 1 & 6 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 9 \\ 8 \\ 0 \end{pmatrix}$$

"Hybrid" Subset Sum Addition Is Also Pseudorandom

1 0 0 1

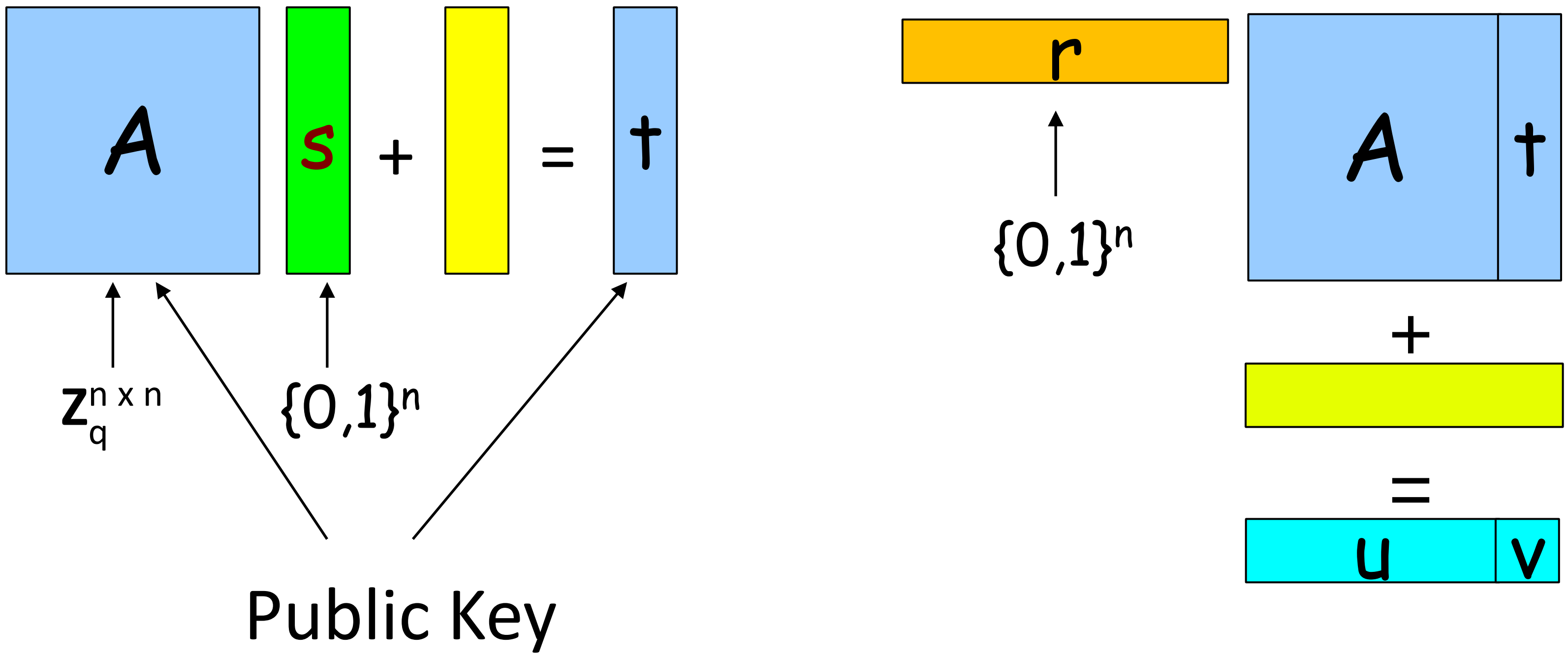
4	6	7	9	0
3	9	0	7	9
8	4	6	5	8
1	6	4	3	0

\+ 1 1 1 0 0

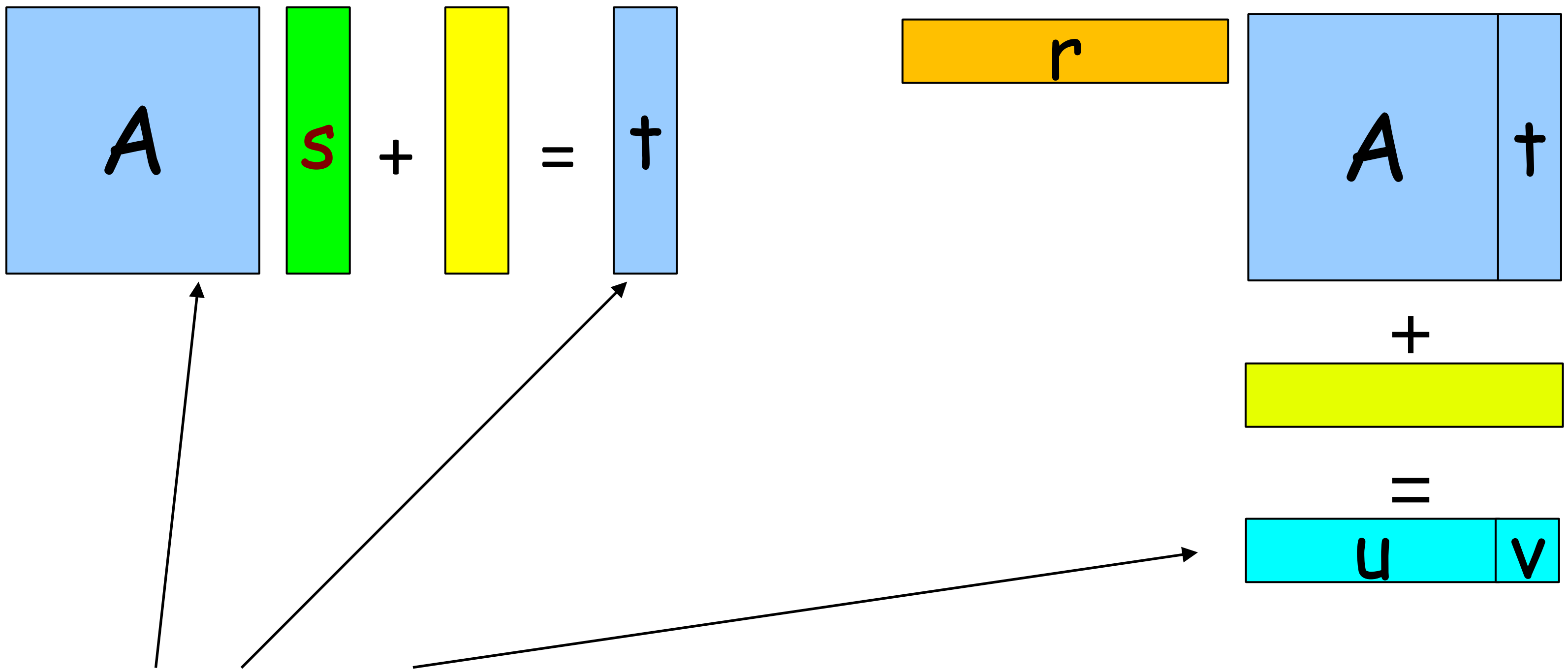
= 6 3 2 2 0

pseudorandom

Encryption Scheme

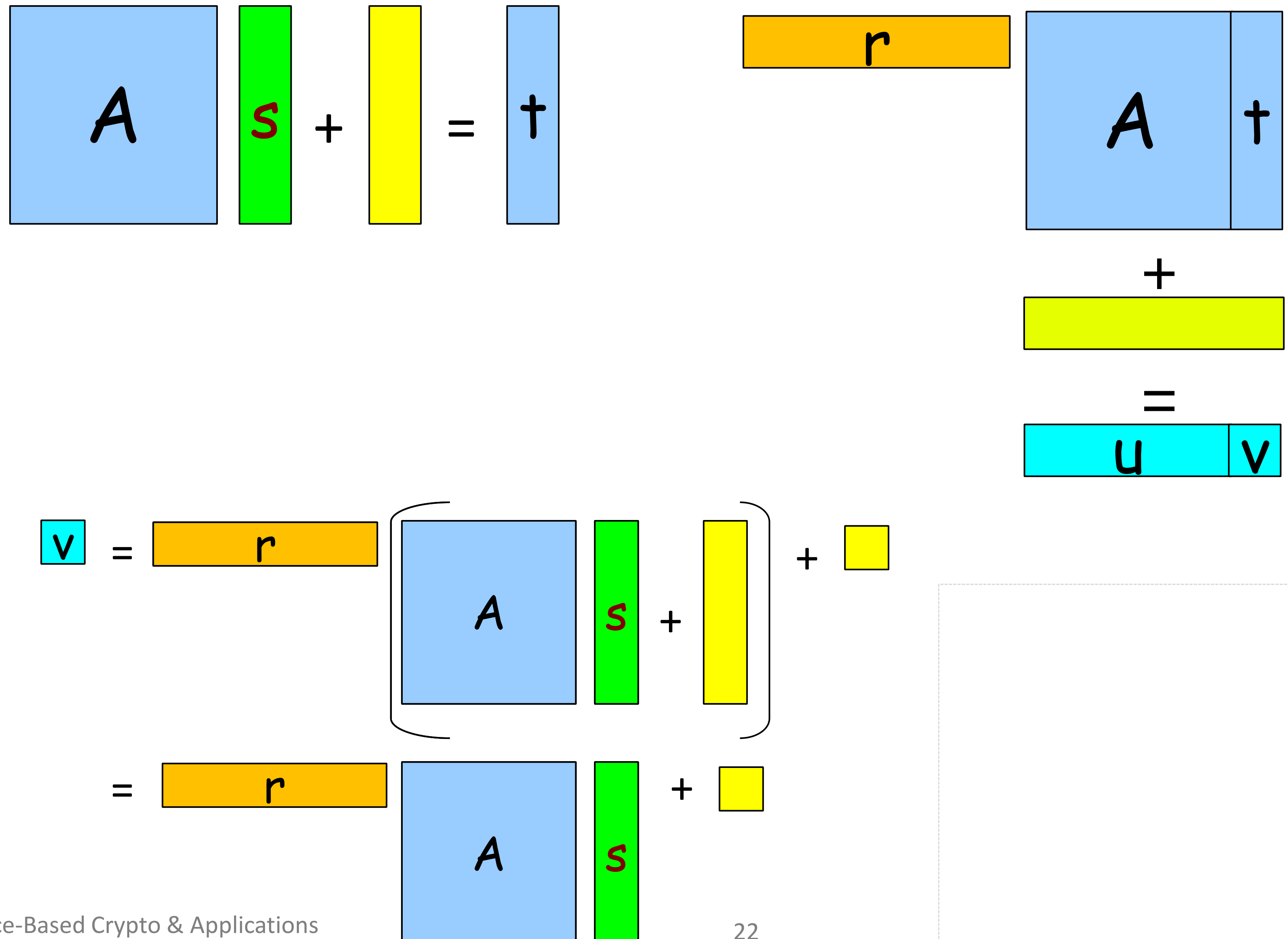


Encryption Scheme

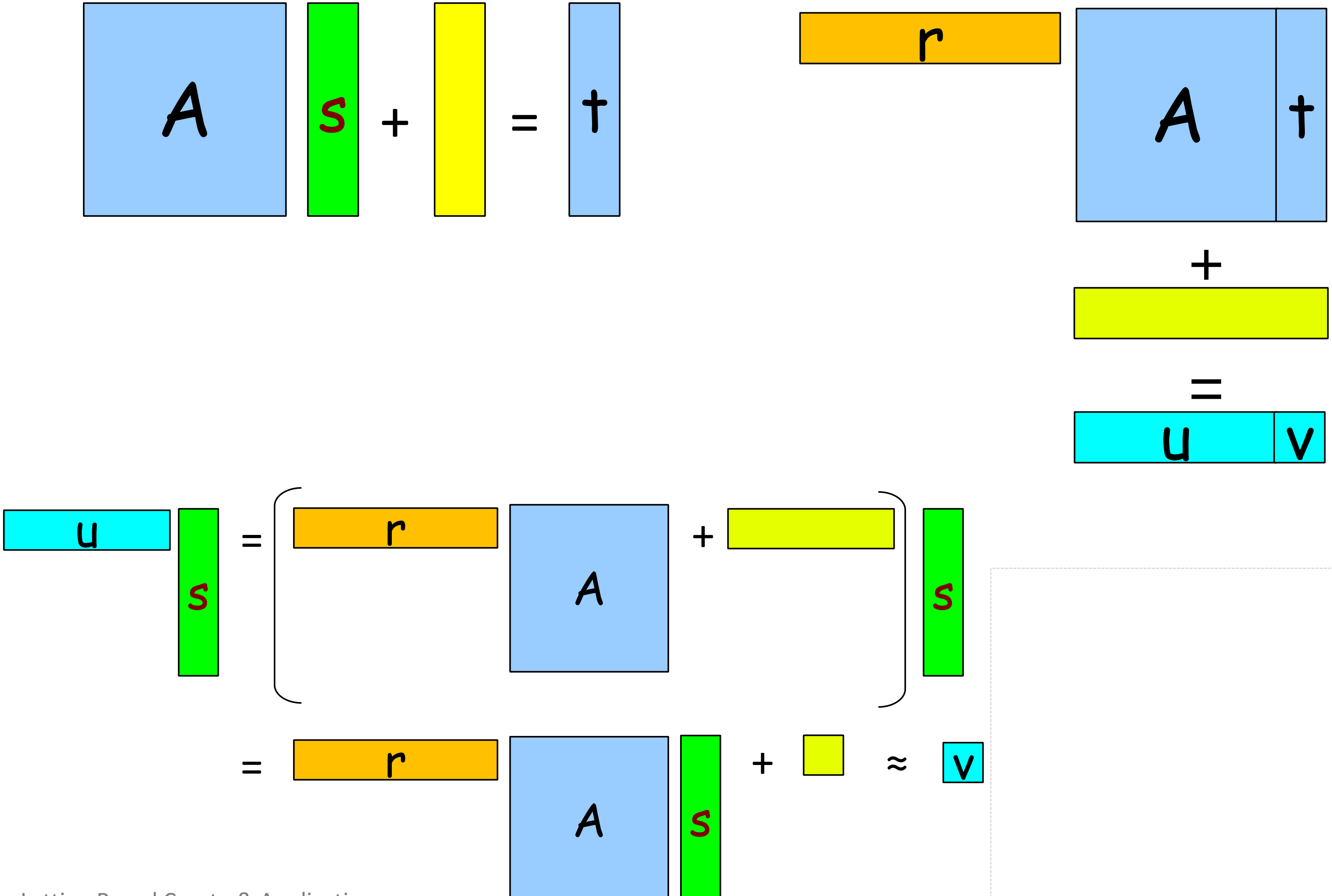


Is pseudo-random based on the hardness of the subset sum problem

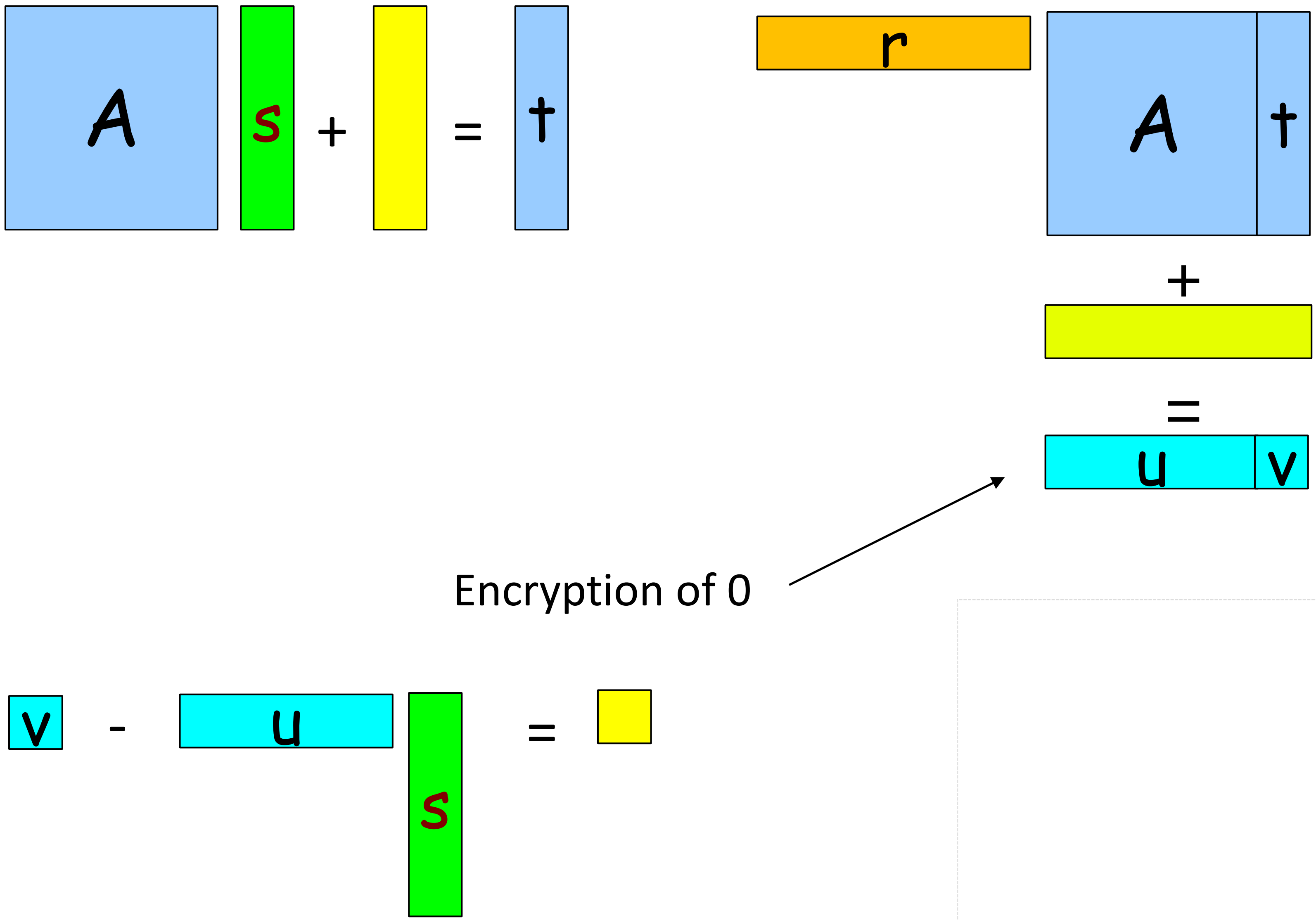
Encryption Scheme



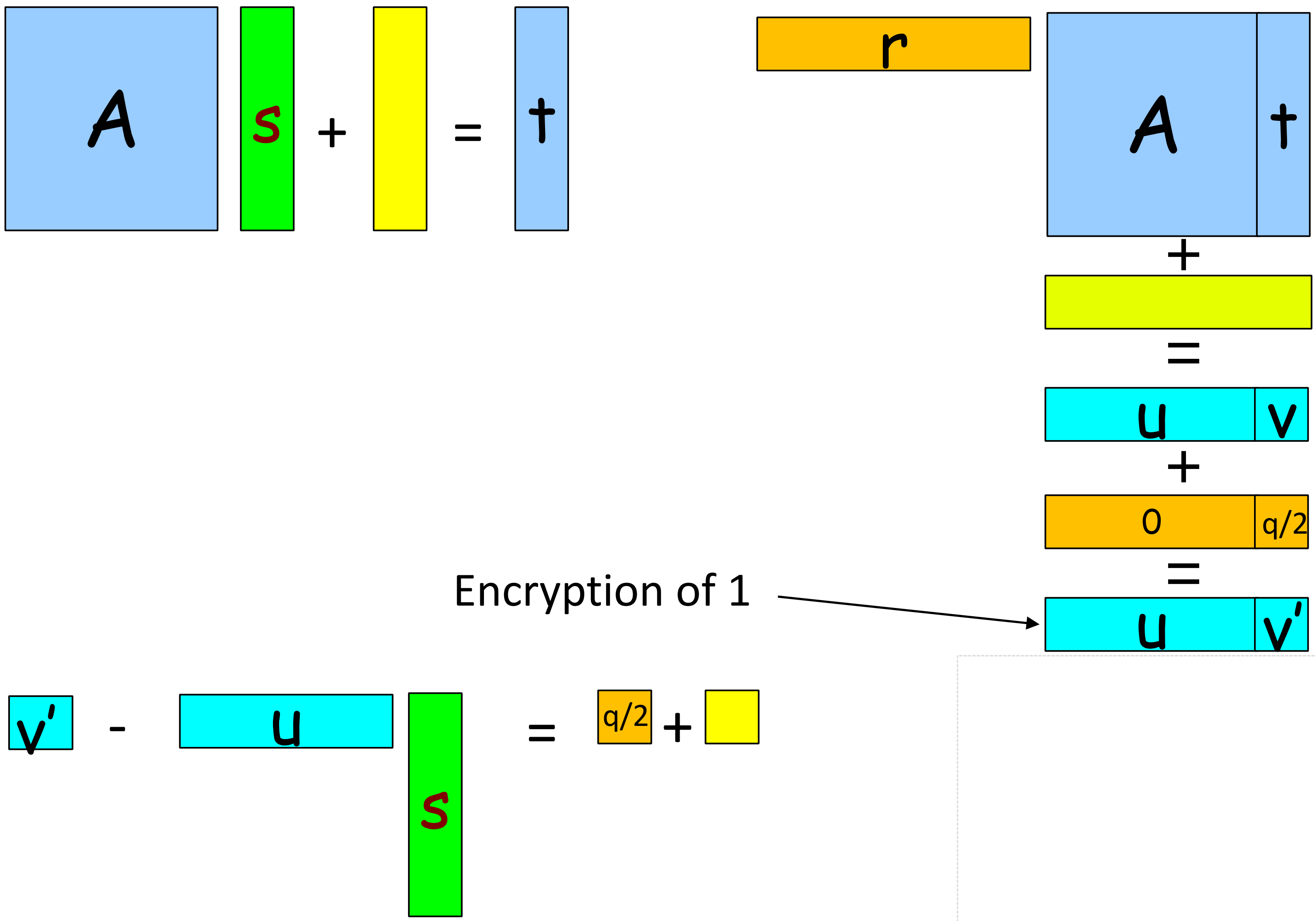
Encryption Scheme



Encryption Scheme



Encryption Scheme

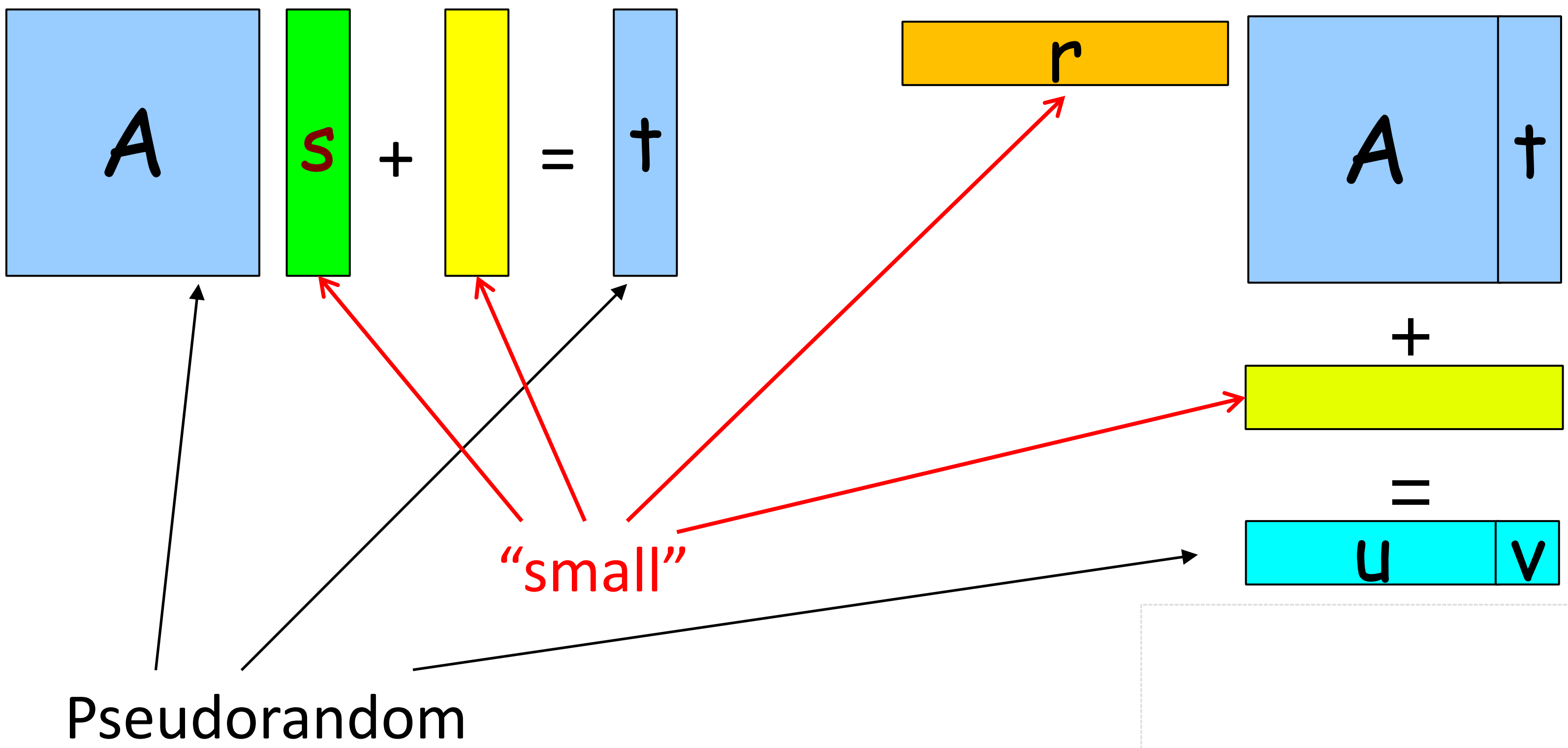


CRYPTOSYSTEM BASED ON LWE

[REGEV 2005]

Encryption Scheme

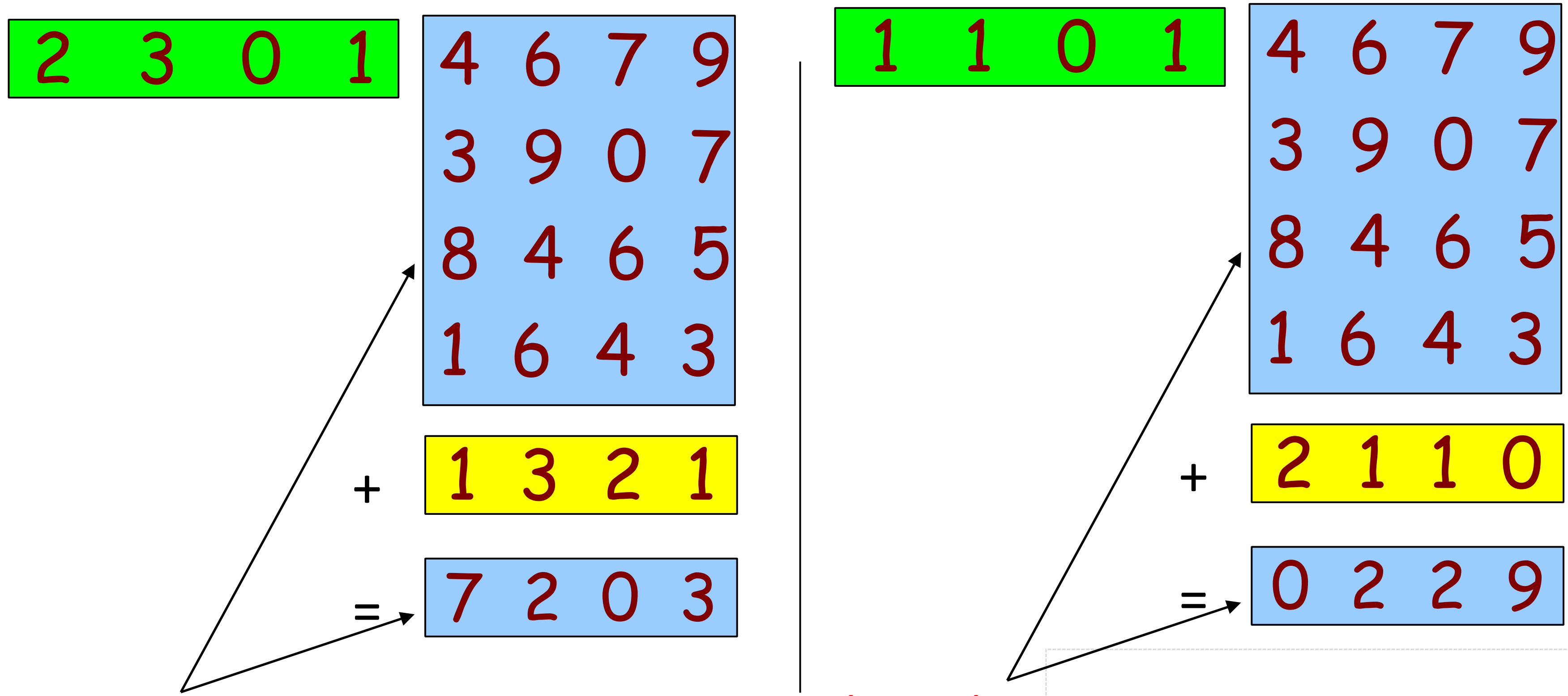
(what we needed)



Picking the “Carries”

- In Subset Sum: carries were deterministic
- What if … we pick the “carries” at random from some distribution?

So…

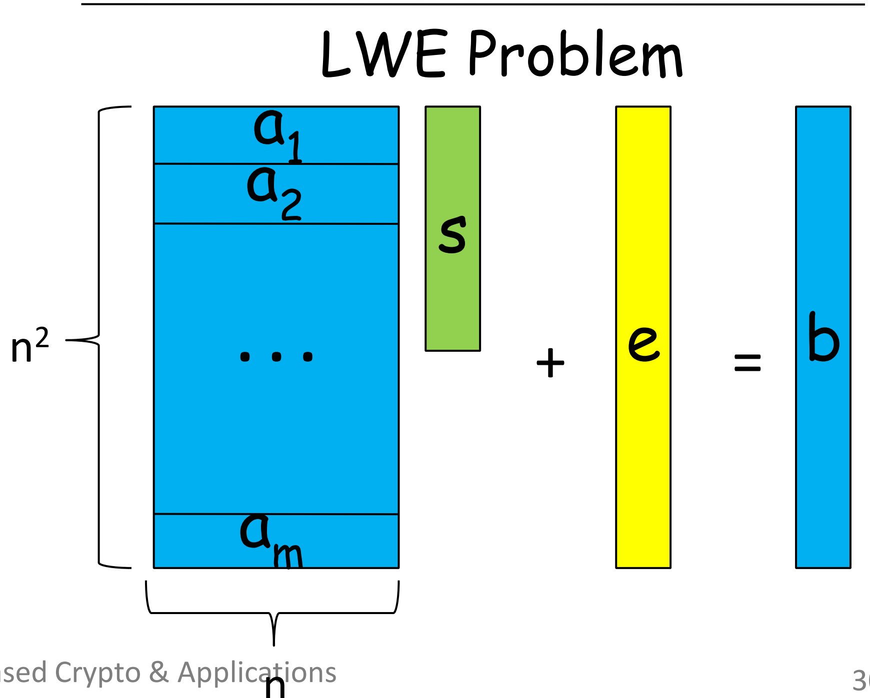


Pseudorandom based on LWE [Reg '05]

Pseudorandom based on Subset Sum

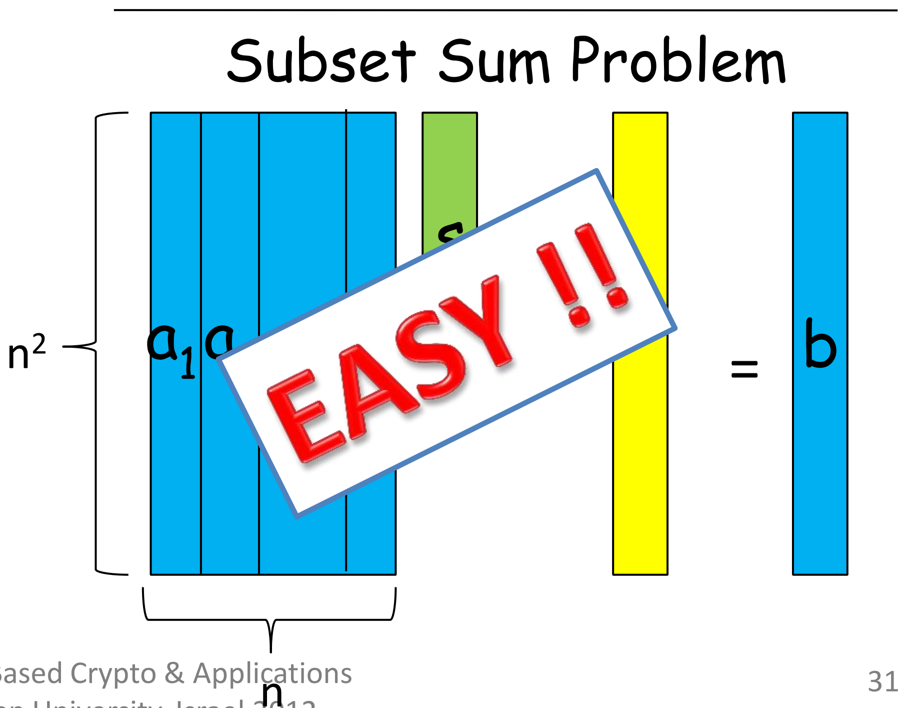
LWE vs. Subset Sum

- The Subset Sum assumption has "deterministic noise"
- The LWE assumption is more "versatile"

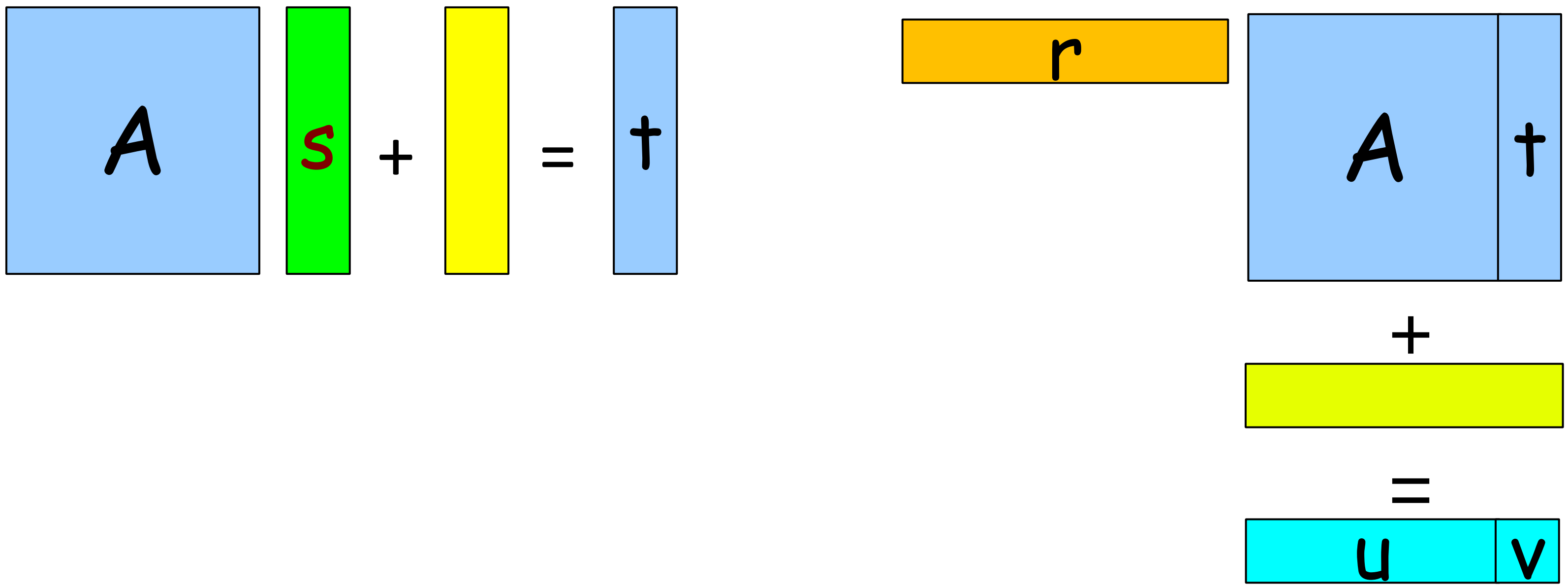


LWE vs. Subset Sum

- The Subset Sum assumption has "deterministic noise"
- The LWE assumption is more "versatile"



LWE / Subset Sum Encryption

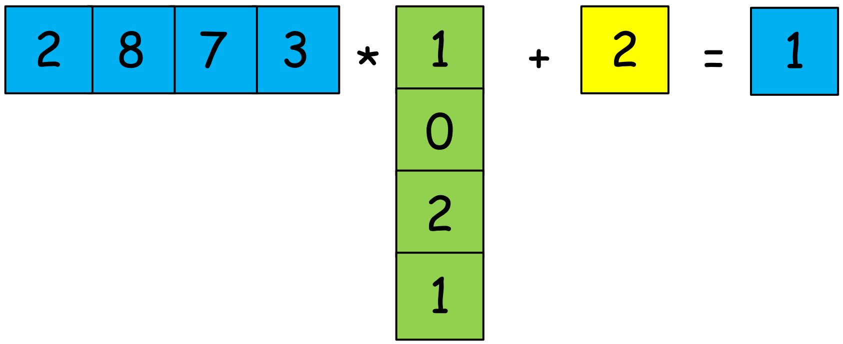


n-bit Encryption	Have	Want
Public Key Size	$\tilde{O}(n)$ / $\tilde{O}(n^2)$	O(n)
Secret Key Size	$\tilde{O}(n)$ / $\tilde{O}(n^2)$	O(n)
Ciphertext Expansion	$\tilde{O}(n)$ / $\tilde{O}(1)$	O(1)
Encryption Time	$\tilde{O}(n^3)$ / $\tilde{O}(n^2)$	O(n)
Decryption Time	$\tilde{O}(n^2)$	O(n)

CRYPTOSYSTEM BASED ON RING-LWE

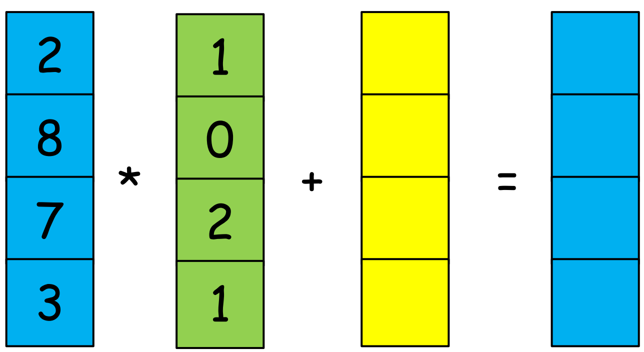
[L, PEIKERT, REGEV 2010]

Source of Inefficiency of LWE



Getting just **one** extra random-looking number requires **n** random numbers and a small error element.

Wishful thinking: get **n** random numbers and produce **n** pseudo-random numbers in “one shot”



Use Polynomials

f(x) is a polynomial $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$

R = $Z_p[x]/(f(x))$ is a polynomial ring with

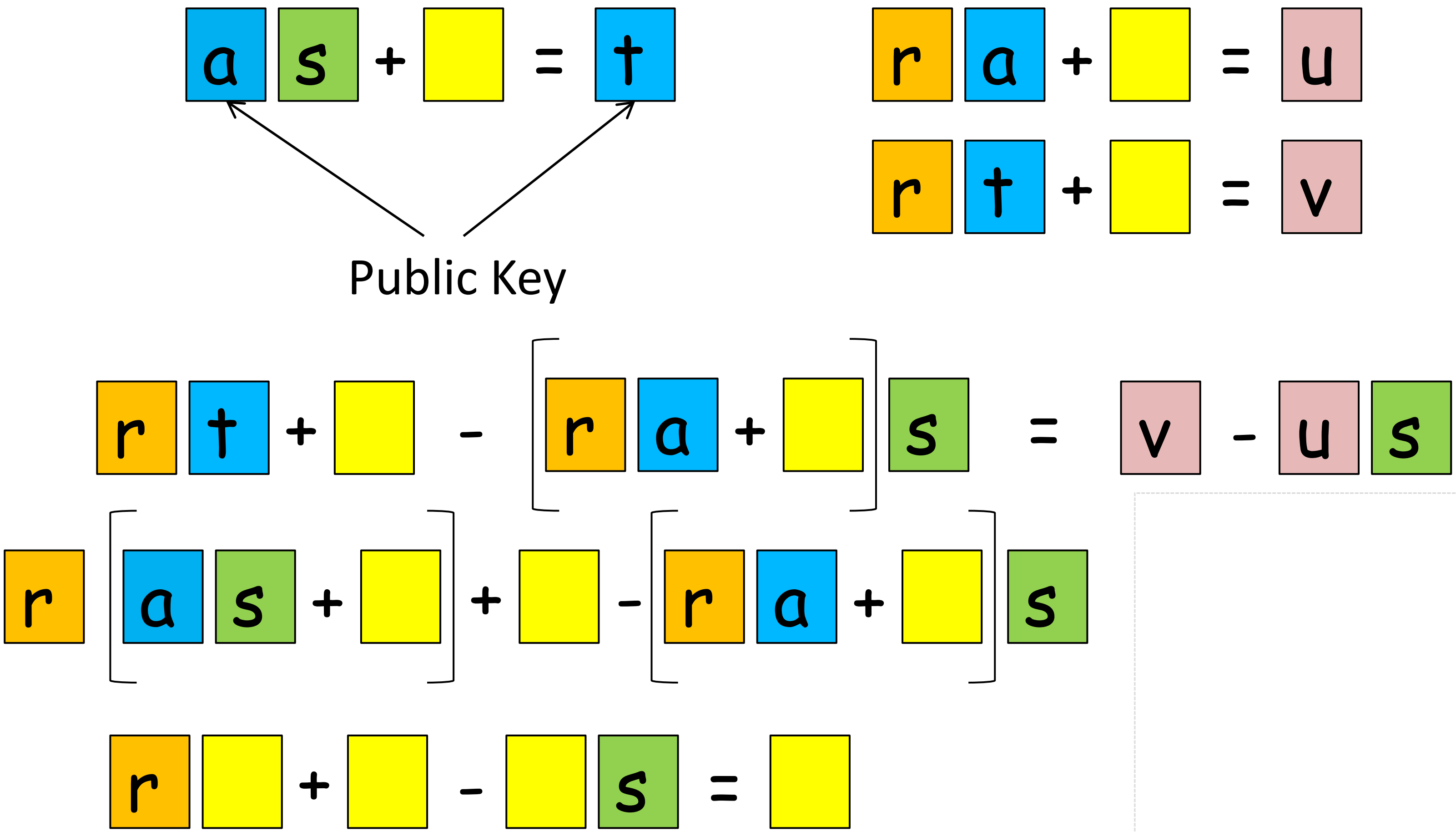
- Addition mod p
- Polynomial multiplication mod p and f(x)

Each element of R consists of n elements in Z_p

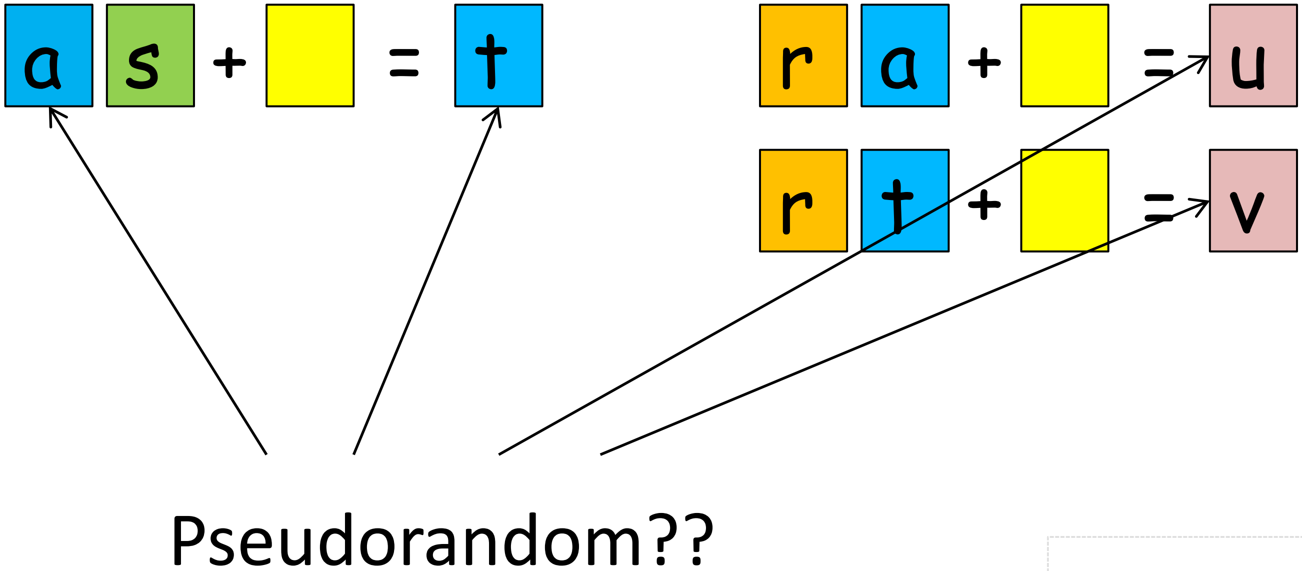
In R:

- small+small = small
- small*small = small (depending on f(x))

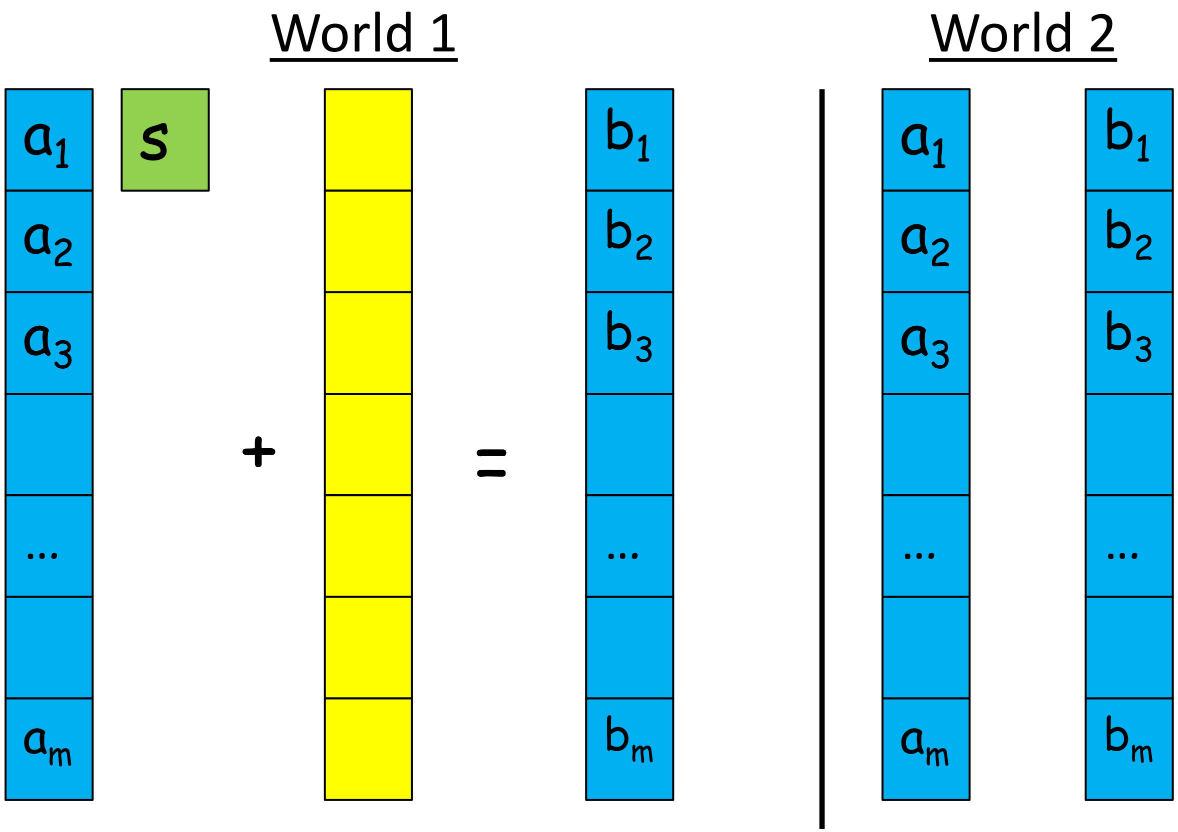
Polynomial Interpretation of the LWE-based cryptosystem



Security



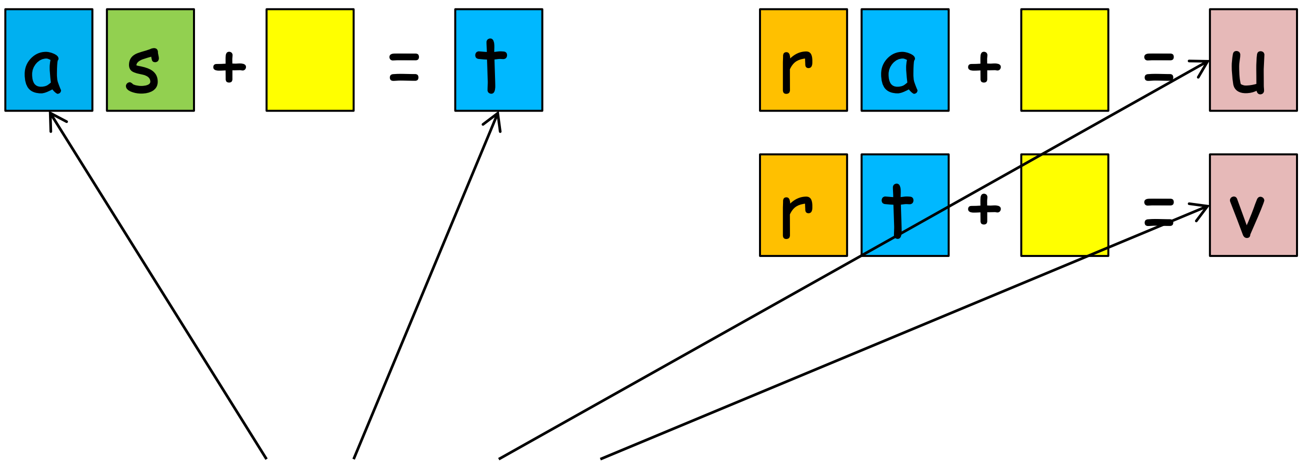
Decision
Learning With Errors over Rings



Theorem [LPR ‘10]: In *cyclotomic* rings,

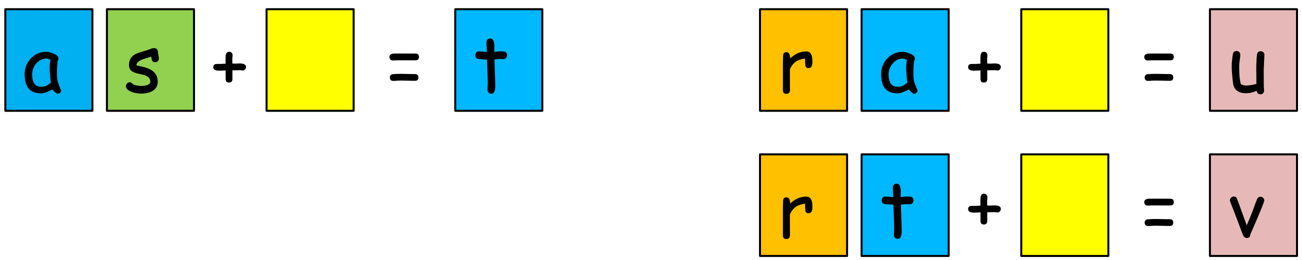
Search-RLWE < Decision-RLWE

Security



Pseudorandom!!

Use Polynomials in $Z_p[x]/(f(x))$



n-bit Encryption	From LWE / SS	From Ring-LWE
Public Key Size	$\tilde{O}(n)$ / $\tilde{O}(n^2)$	$\tilde{O}(n)$
Secret Key Size	$\tilde{O}(n)$ / $\tilde{O}(n^2)$	$\tilde{O}(n)$
Ciphertext Expansion	$\tilde{O}(n)$ / $\tilde{O}(1)$	$\tilde{O}(1)$
Encryption Time	$\tilde{O}(n^3)$ / $\tilde{O}(n^2)$	$\tilde{O}(n)$
Decryption Time	$\tilde{O}(n^2)$	$\tilde{O}(n)$

1-ELEMENT CRYPTOSYSTEM BASED ON RING-LWE

[STEHLE, STEINFELD 2011]

Number of Ring Elements

$a \; s + \square = t$

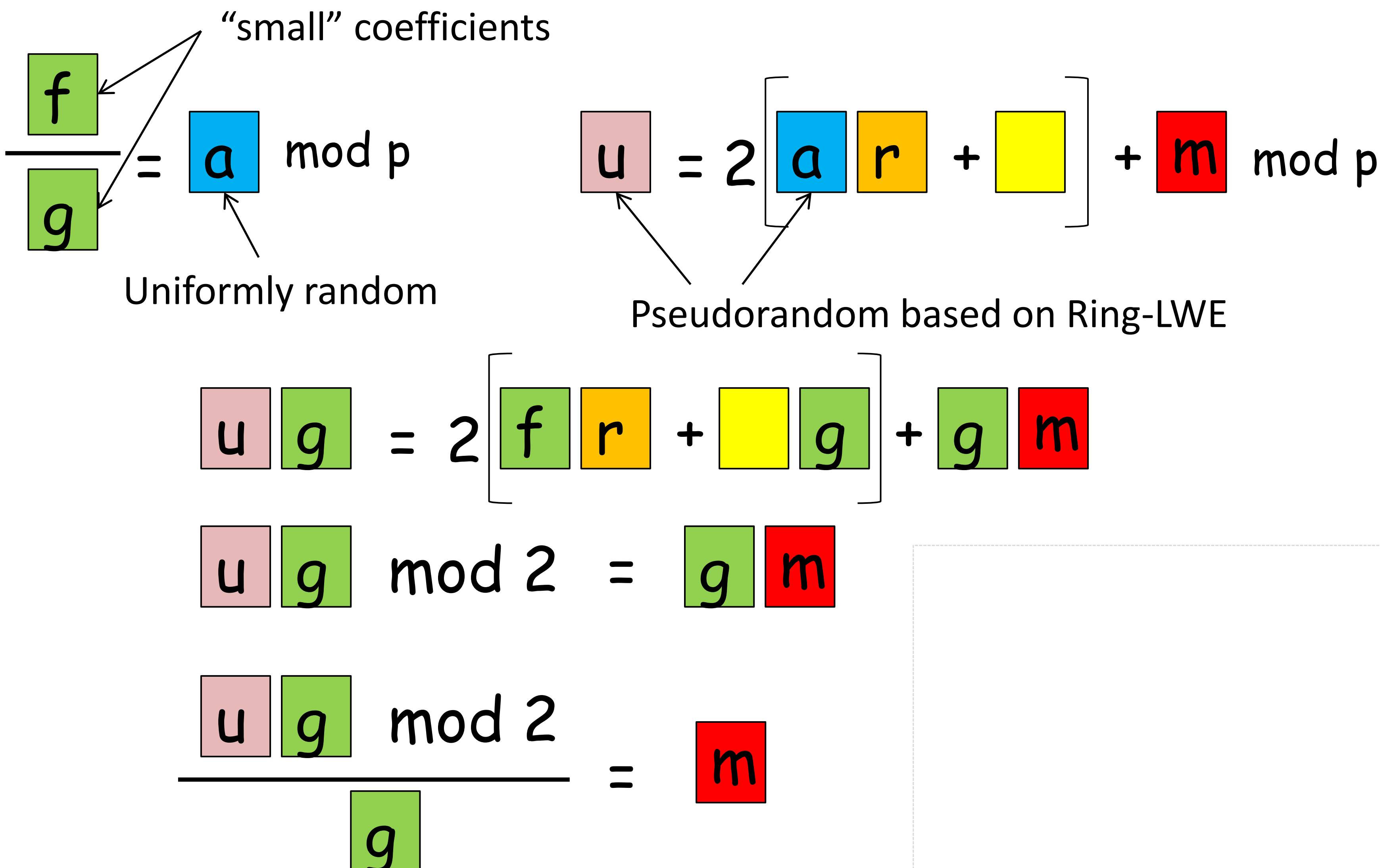
$r \; a + \square = u$

$r \; t + \square = v$

Encryption of m: $u \; , \; v + \frac{p}{2} m$

Can you have a ciphertext with just 1 ring element?

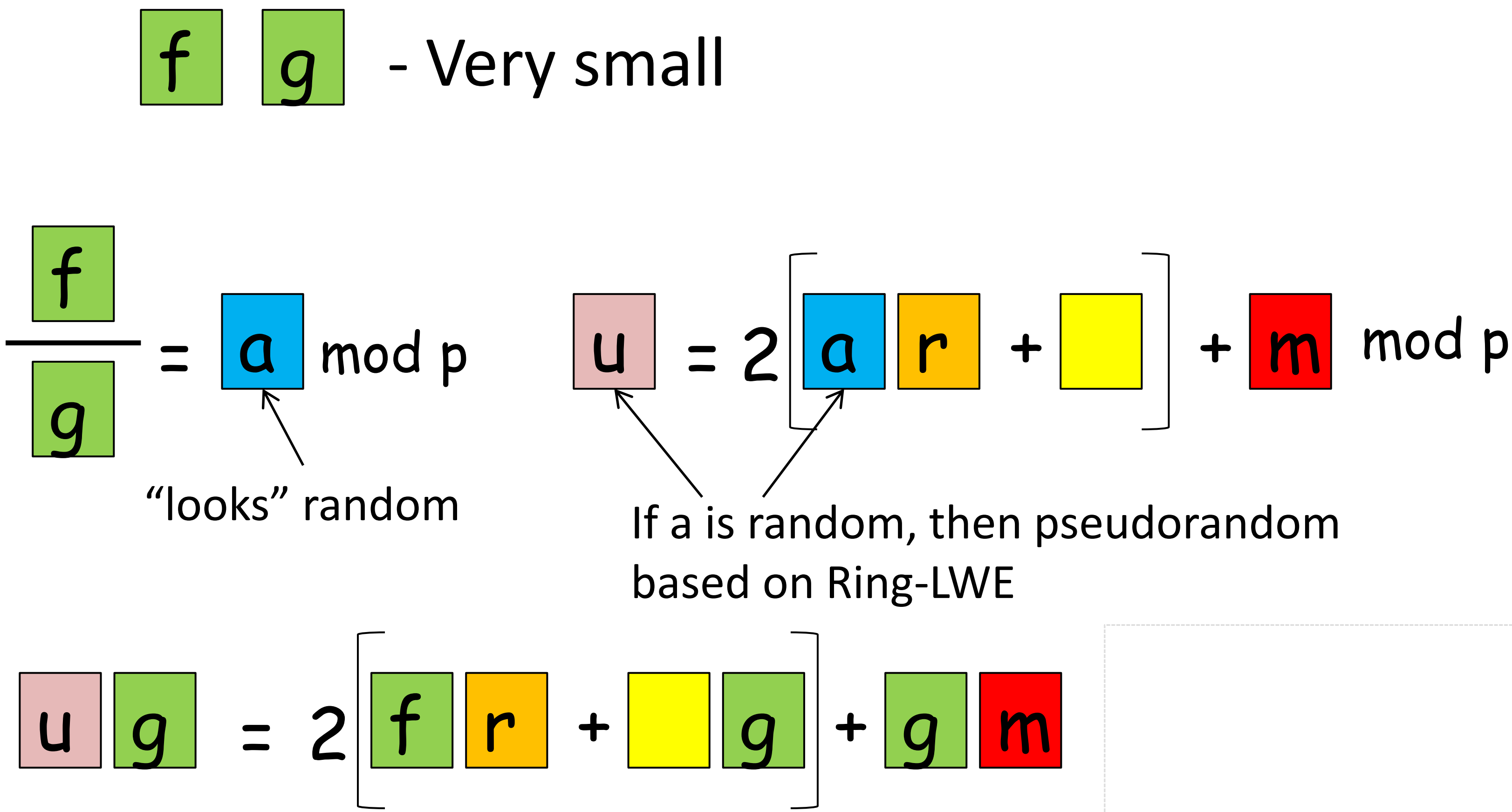
Stehle, Steinfeld Cryptosystem



NTRU CRYPTOSYSTEM

[HOFFSTEIN, PIPHER, SILVERMAN 1998]

NTRU Cryptosystem



Since f, g are smaller, p can be smaller as well

(Textbook) NTRU Cryptosystem / Trap-Door Function

f g - Very small

$$\frac{f}{g} = a \bmod p \qquad u = 2ar + m \bmod p$$

$$u\,g = 2fr + gm$$

$$u\,g \bmod 2 = gm$$

$$\frac{u\,g \bmod 2}{g} = m$$

References

- Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman (1998): NTRU: A Ring-Based Public Key Cryptosystem
- Oded Regev (2005): On lattices, learning with errors, random linear codes, and cryptography
- Vadim Lyubashevsky, Adriana Palacio, Gil Segev (2010): Public-Key Cryptographic Primitives Provably as Secure as Subset Sum
- Vadim Lyubashevsky, Chris Peikert, Oded Regev (2010): On Ideal Lattices and Learning with Errors over Rings
- Damien Stehlé, Ron Steinfeld (2011): Making NTRU as Secure as Worst-Case Problems over Ideal Lattices