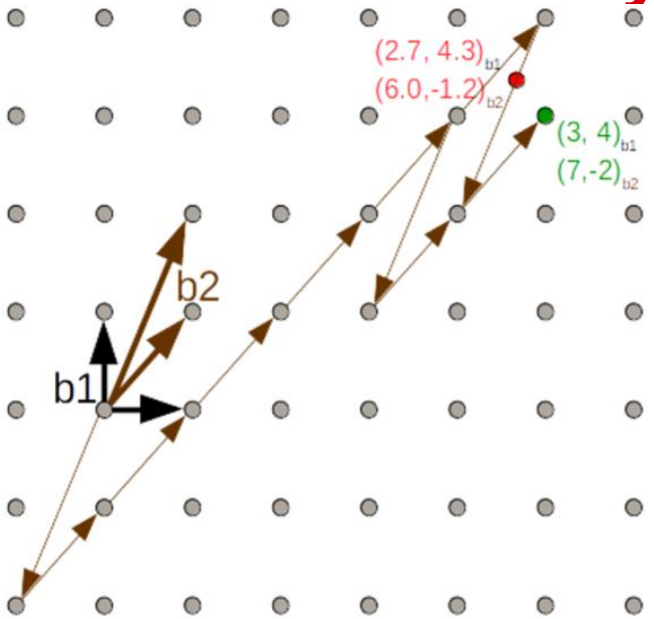
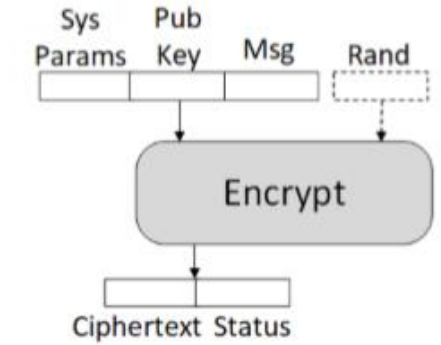
Physical Protection of Lattice-Based Cryptography – Challenges and Solutions

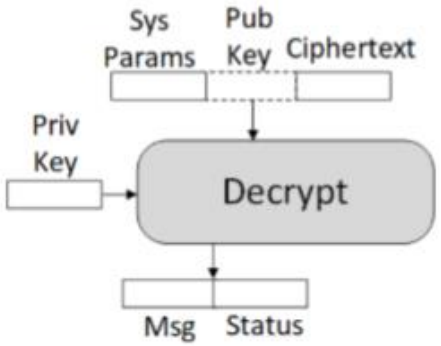
DR. AYESHA KHALID

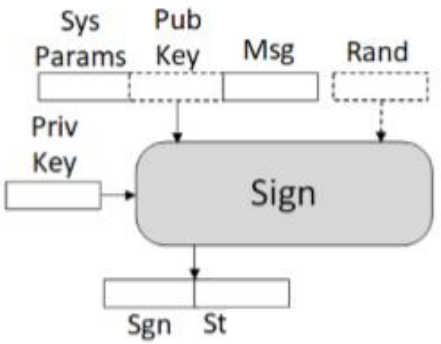
NOVEMBER 2018

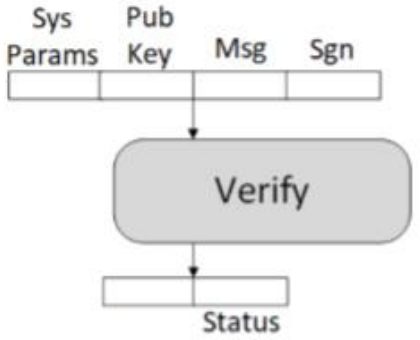
Lattice based Cryptography











Security

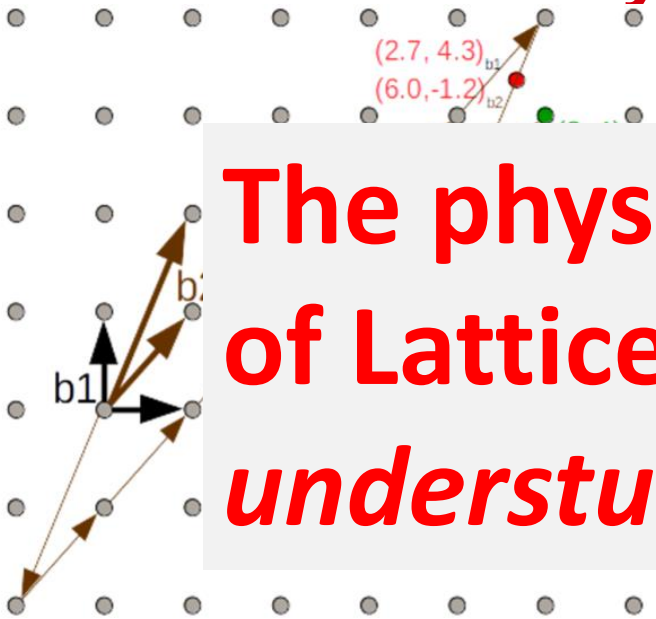
Efficiency

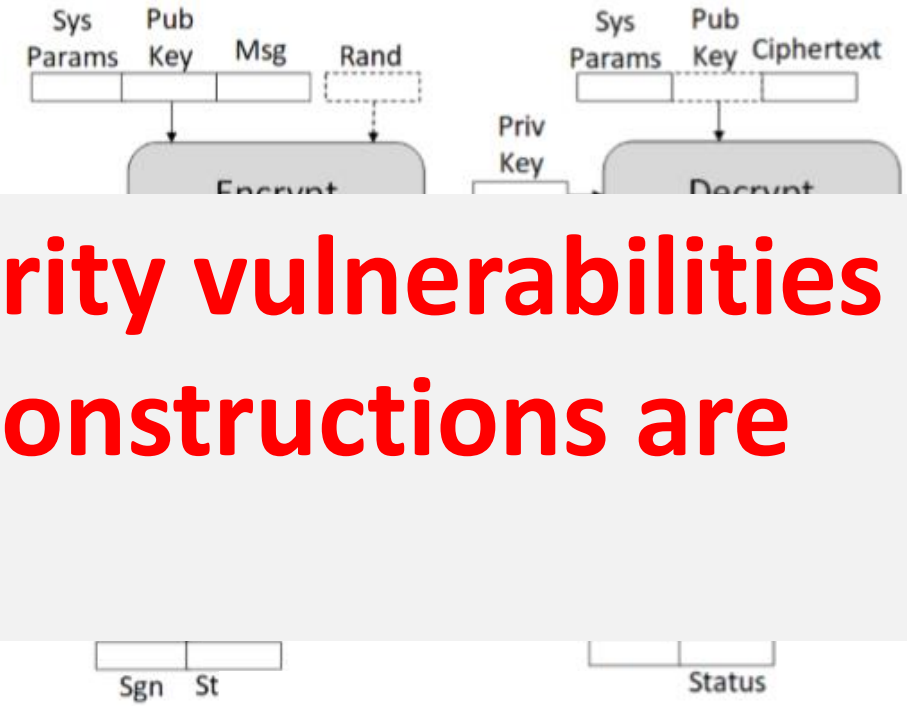
Versatility

Family	Signature	Encryption/ KEM	Total
Lattice-based	5	23	28
Code-based	3	17	20
Multivariate	8	2	10
Hash-based	3	0	3
Isogeny-based	0	1	1
Other	2	5	7
Total	21	48	69

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Lattice based Cryptography





- ✓ Security
- ✓ Efficiency
- ✓ Versatility

The physical security vulnerabilities of Lattice based constructions are *understudied !!!*

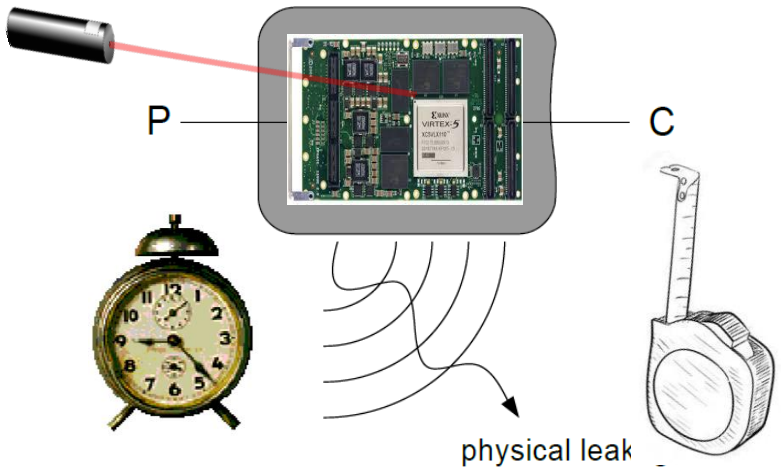
Fami			
Latti			
Code			
Mult			
Hash-based	3	0	3
Isogeny-based	0	1	1
Other	2	5	7
Total	21	48	69

"Schemes that can be made resistant to SCA attacks **at minimal cost are more desirable** than those whose performance is severely hampered by any attempt to resist SCA " [1]

NIST

[1] http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-forproposals-final-dec-2016.pdf

Side Channel Analysis (SCA) attacks on LBC



LBC Ingredients

- **Matrix vector multiplication (**for standard lattices)
- **Polynomial multiplication** (for ideal lattices)
- **RNGs/ XOFs/ Hashes**
- **Error Sampling**
  - •Discrete Gaussian sampling
  - •Binomial distribution

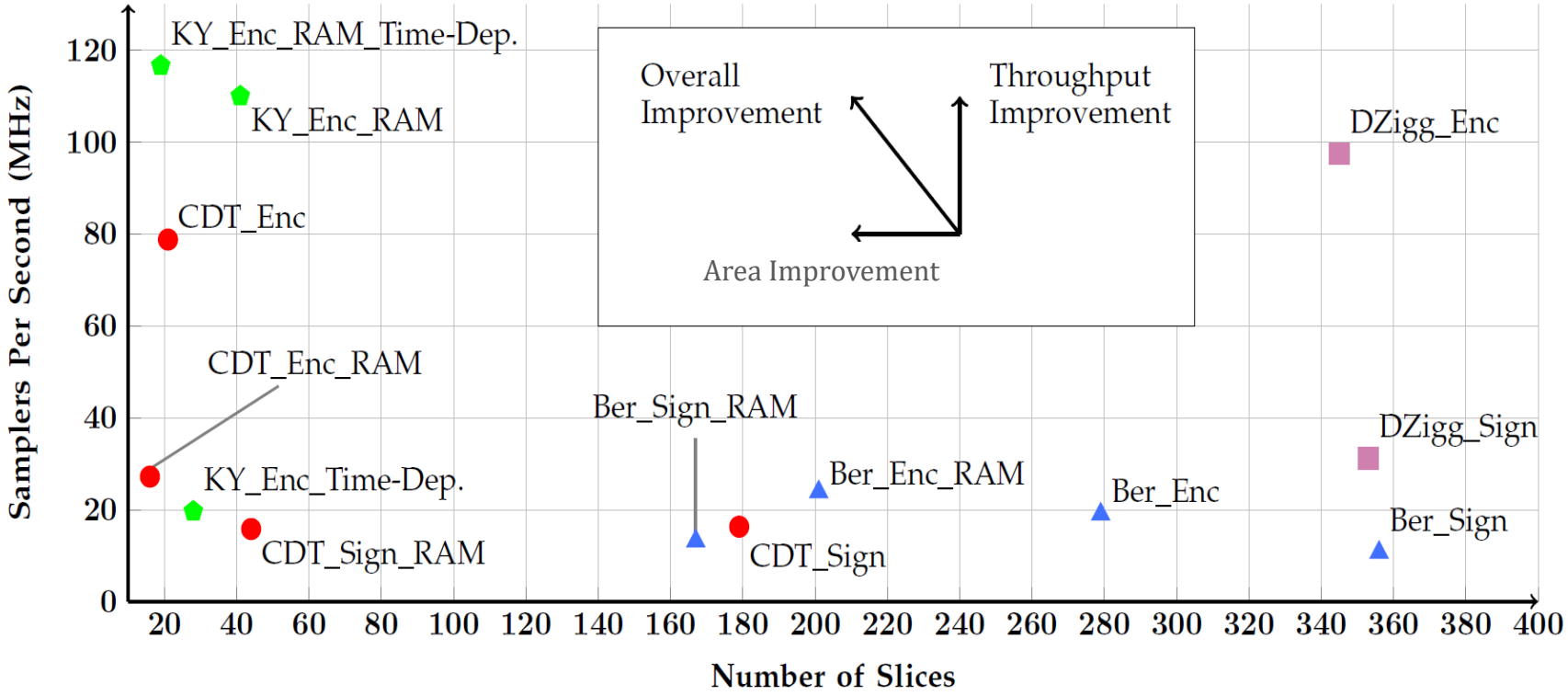
LATTICE-BASED KEY ENCAPSULATION (KEM) AND SIGNATURE SCHEMES SUBMITTED TO NIST FOR POST-QUANTUM STANDARDISATION, SEPARATED BY THEIR NIST SECURITY LEVELS, ERROR TYPE (GAUSSIAN OR BINOMIAL), AND PARAMETER VALUE (FOR ALL SCHEMES $\mu = 0$).

Crypto. Type	Cryptographic Scheme	Security Level	Error Type	Error Parameter (σ)
KEM	Ding Key Ex. [DTGW17]	1,3,5	G	2.6, 4.19
	(R-)EMBLEM [SPL+17]	1	G	25, 3
	FrodoKEM [NAB+17]	1,5	G	2.75, 2.3
	Kyber [SAB+17]	1,3,5	B	$\sqrt{2}$
	LAC [LLJ+17]	1,3,5	B	$1/\sqrt{2}, 1/2$
	LIMA [SAL+17]	3	B	3.16
	Lizard [CPL+17]	1,5	G	≈ 2
	LOTUS [PHAM17]	1,2,3,4,5	G	3
	KCL [ZjGS17]	3,5	B	$\sqrt{8}, \sqrt{6}$
	NewHope [PAA+17]	1,3	B	2
	NTRU-RSS-KEM [SHRS17]	1	B	1
	NTRUEncrypt [ZCHW17a]	1,3,5	G	724
	Mersenne-756839 [AJPS17]	1	G	28.64
	Titanium [SSZ17]	1,3,5	B	$\sqrt{2}$
Sign-ature	Dilithium-G [LDK+17]	1,2,3	G	19200, 17900,12400
	Falcon [PFH+17]	1,2,3,4,5	G	171.8, 213.1
	pqNTRUSign [ZCHW17b]	1	G	107
	qTESLA [BAA+17]	1,3,5	B	8.5, 10

Independent time Gaussian error samplers on custom hardware

Error Sampling has been targeted for noticeable timing/ cache attacks

- Comprehensive evaluation of Discrete Gaussian Samplers - offers recommendations on most appropriate sampler to use for encryption, authentication, high-speed applications etc..
- Proposed independent-time hardware designs of a range of samplers offering security against side-channel timing attacks



CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Protecting error samplers against Fault injection attacks

Test Level	Test Description	Test Formula
Low Cost	Check for repetitions	A counter for if $x_i = c$
Standard	Sample Mean ($\bar{x}$)	$(\sum_{i=1}^{n} x_i)/n$
	Sample Variance ($\bar{s}$)	$(\sum_{i=1}^{n} x_i^2 - (\sum_{i=1}^{n} x_i)^2)/n$
	Standard Error of $\bar{x}$	$\mathrm{SE}_{\bar{x}} = \bar{s}/\sqrt{n}$
	Test Statistic for $\bar{s}$	$T = (n/s)\bar{s}$
	Null Hypothesis	Check if $\lvert\mu\rvert < \bar{x} + t_{\alpha/2}\mathrm{SE}_{\bar{x}}$
	Null Hypothesis	Check if $T < \hat{\chi}^2_{n,\alpha/2}$
Expensive	Chi-Squared Test	$\hat{\chi}^2 = \sum_{k=1}^{n} \frac{(\mathrm{obs}(k) - \exp(k))^2}{\exp(k)}$
	Test Statistic for $\hat{\chi}^2$	$\chi^2(df = n-1, p\text{-value})$
	Null Hypothesis	Check if $\hat{\chi}^2 < \chi^2(n-1, 0.99)$

Increasingly powerful statistical analysis tests to detect increasingly sophisticated fault injection attacks including

- ***zeroing attacks***
- ***randomization***
- ***early loop abort***

Countermeasure Category	LUT/FF	Slices	DSP/ BRAM	Freq. (MHz)	Clock Cycles	Ops/sec ($\times 10^6$)
Plain CDT Sampler	115/81	33	0/0	297	6	49.5
Low Cost	6/10	3	0/0	-	$+0^{\dagger}$	-
CDT with Low Cost	123/91	36	0/0	297	6	49.5
Standard	74/58	24	0/0	-	$+1^{\dagger}$	-
CDT with Standard	182/139	55	0/0	297	6	49.5
Expensive	226/436	126	1/0	-	$+32^{\dagger}$	-
CDT with Expensive	315/517	149	1/0	297	6	49.5
CDT with Expensive	251/453	129	1/1	193	6	38.6

8%

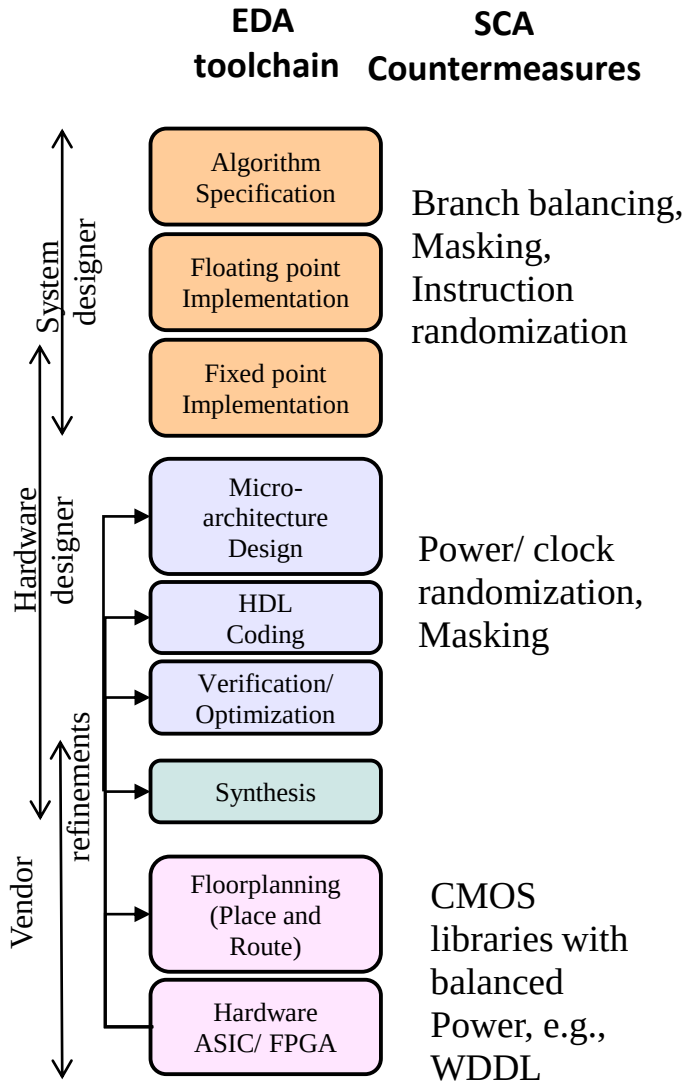
44%

400%

Resource overhead

†This is a one-off clock cycle count at the end of n samples, whereas others are clock cycles per sample.

Addressing SCA countermeasures for LBC



- **Open Questions**
  - Modelling/profiling of SCA Leakage for LBC schemes. *Evaluating SCA-vulnerability*

    Which schemes/ underlying modules are naturally least SCA-vulnerable? Application recommendations…

  - Early warning signs detection by at higher abstraction level by a formal treatment of SCA leakages.
  - EDA aided user directed SCA countermeasures insertion.
  - Multiple SCA countermeasures are not studied *together*, e.g., masking+parity checks=new vulnerability?

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Thank you

Questions?

CSIT
CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES