From: Alagic, Gorjan (Assoc)
To: (b) (6)
Subject: FW: Slides for LUOV and Rainbow
Date: Tuesday, April 30, 2019 9:27:00 AM
Attachments: LUOV and Rainbow.pptx

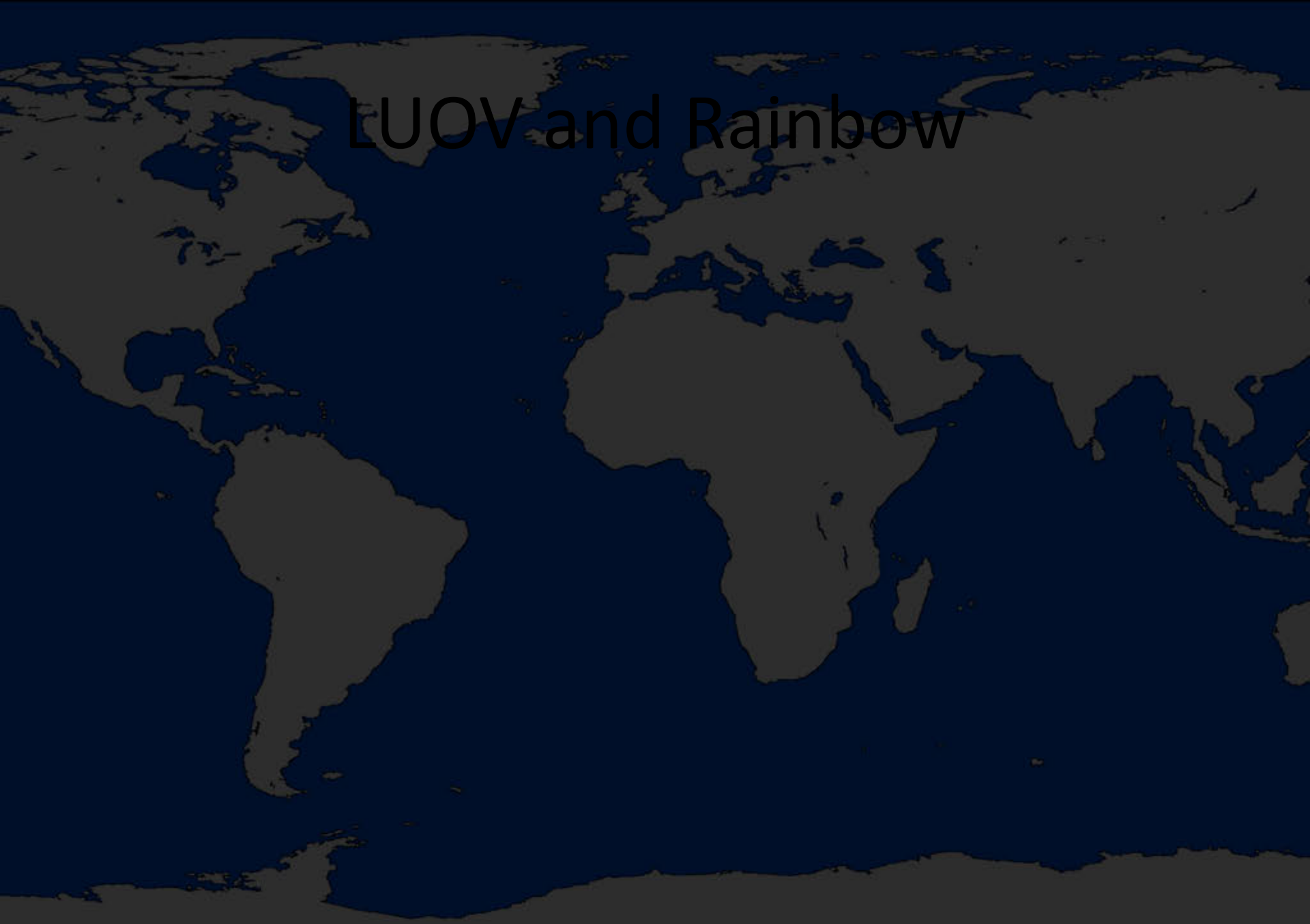
From: Smith-Tone, Daniel (Fed)
Sent: Tuesday, April 30, 2019 9:16 AM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Slides for LUOV and Rainbow

Hello, fellow members of my species,

Please find attached the slides we plan to use in our PQC meeting today. With any luck, we will not experience an extinction level event before we meet, rendering these slides useless. Yes. Extinction level event after meeting = much better.

Cheers!
Daniel the elder

LUOV and Rainbow



LUOV

- Based on the oil-vinegar signature scheme
- Algebraically, LUOV is basically the same as UOV, which has been studied since 1998
- Introduces a new “field lifting” modification that is original and exciting, but unstudied
- Round 2 version incorporates random salts and randomizes vinegar variable selection
- Still maintains a message recovery mode

Oil-Vinegar

Let $\mathbb{F}$ be a finite field with q elements. Fix an integer v and set $n = 2v$.

Define $F: \mathbb{F}^n \to \mathbb{F}^v$ by

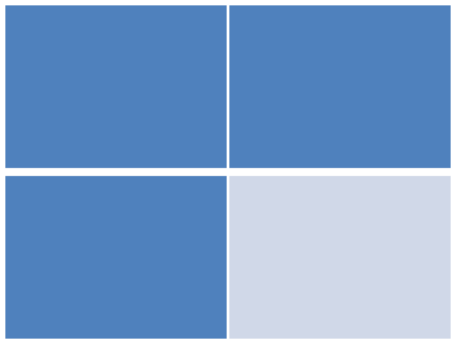
$$F_l(\boldsymbol{x}) = \sum_{i=1}^{v} \sum_{j=i}^{n} \alpha_{ijl} x_i x_j + \sum_{i=1}^{n} \beta_{il} x_i + \gamma\_l$$

Finally, let $L: \mathbb{F}^n \to \mathbb{F}^n$ be affine and define

$$P(\boldsymbol{x}) = F \circ L(\boldsymbol{x}).$$

Structure of Quadratic Forms

$$F_l = \begin{bmatrix} \alpha_{11l} & \cdots & \alpha_{1vl} & \alpha_{1(v+1)l} & \cdots & \alpha_{1nl} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{1vl} & \cdots & \alpha_{vvl} & \alpha_{v(v+1)l} & \cdots & \alpha_{vn1} \\ \alpha_{1(v+1)l} & \cdots & \alpha_{v(v+1)l} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & 0 \\ \alpha_{1nl} & \cdots & \alpha_{vnl} & 0 & \cdots & 0 \end{bmatrix}$$



Unbalanced Oil-Vinegar (UOV)

Fix integers o and v and set $n = o + v$. Define the map $F: \mathbb{F}^n \to \mathbb{F}^o$ by

$$F_l(\boldsymbol{x}) = \sum_{i=1}^{v} \sum_{j=i}^{n} \alpha_{ijl} x_i x_j + \sum_{i=1}^{n} \beta_{il} x_i + \gamma\_l$$

Fix an affine map $L: \mathbb{F}^n \to \mathbb{F}^n$ and define

$$P(\boldsymbol{x}) = F \circ L(\boldsymbol{x}).$$

Field Lifting

- LUOV = Lifted UOV
- The public key is defined over $\mathbb{F}_2$ but the multivariate ring $\mathbb{F}_2[\boldsymbol{X}]$ is embedded in $\mathbb{F}_{2^r}[\boldsymbol{X}]$
- UOV structure is the same
- Parameters still selected so that solving $P(\boldsymbol{x}) = \boldsymbol{y}$ is hard even when $x_i, y_i \in \mathbb{F}_2$.

Inversion of the Central Map

To find a preimage $\boldsymbol{x}$ of $\boldsymbol{y}$ under P, solve the linear system

$$\boldsymbol{y} = F(\boldsymbol{v}, \boldsymbol{u})$$

for $\boldsymbol{u}$ where $\boldsymbol{v}$ is random of dimension v.

Then solve $\boldsymbol{v} \parallel \boldsymbol{u} = L(\boldsymbol{x})$.

- This process is probabilistic
- Failure probability is about 2^{-r}.

On Side-Channel Leakage

- Claim that constant-timeness of AVX2 implementation is “verified” by a couple of tools, Valgrind and dudect
- Admit that the Valgrind test fails specifically by leaking number of signing attempts made
- No direct leakage of secret information

LUOV Parameter Sets

	claimed security level	r	m	v	SHAKE	|sig|	|pk|	|sk|	message recovery (optional)
LUOV-8-58-237	lvl 2	8	58	237	128	311 B	12.1 KB	32B	25 B
LUOV-8-82-323	lvl 4	8	82	323	256	421 B	34.1 KB	32B	17 B
LUOV-8-107-371	lvl 5	8	107	371	256	494 B	75.5 KB	32B	42 B
LUOV-48-43-222	lvl 2	48	43	222	128	1606 B	5.0 KB	32B	225 B
LUOV-64-61-302	lvl 4	64	61	302	256	2904 B	14.1 KB	32B	423 B
LUOV-80-76-363	lvl 5	80	76	363	256	4390 B	27.1 KB	32B	695 B

AVX2 Optimized Performance

	security level	PRNG	keygen (cycles)	sign (cycles)	verify (cycles)
LUOV-8-58-237	2	Keccak	2.5 M	1.7 M	1.3 M
		Chacha8	1.4M	660 K	250 K
LUOV-8-82-323	4	Keccak	7 M	3.6 M	2.8 M
		Chacha8	5.6 M	1.8 M	960 K
LUOV-8-107-371	5	Keccak	12 M	5.7 M	4.1 M
		Chacha8	9.6 M	3.1 M	1.5 M

AVX2 Performance w/ Precomputation

	security level	PRNG	precompute sk	precompute pk	sign	verify
LUOV-8-58-237	2	Keccak Chacha8	3.7 M 2.7 M	1.2 M 204 K	235 K	71 K
LUOV-8-82-323	4	Keccak Chacha8	11 M 9.5 M	2.6 M 922 K	659 K	290 K
LUOV-8-107-371	5	Keccak Chacha8	18 M 16 M	3.9 M 1.7 M	958 K	454 K

Offline Signing Precomputation

- Implemented an additional offline signing precomputation mode
- Utilizes the fact that signature generation consists of:
  - Select a random $\boldsymbol{v}$.
  - Generate linear system $\boldsymbol{y} = F(\boldsymbol{v}, \cdot)$
  - Apply L^{-1}.
- Probably a bad idea.

Security Analyses

		Direct forgery		UOV attack		Reconciliation attack	
(r, m, v)	security	optimal k	complexity	classical	quantum	classical	quantum [1]
$(8, 58, 237)$	lvl 2	2	146	210	146	177	173
$(8, 82, 323)$	lvl 4	3	212	274	210	242	259
$(8, 107, 371)$	lvl 5	4	273	298	234	278	307
$(48, 43, 222)$	lvl 2	1	147	210	146	166	158
$(64, 61, 302)$	lvl 4	1	214	274	210	226	238
$(80, 76, 363)$	lvl 5	1	273	321	257	299	335

Changes from Round 1

- Smaller security margin. They say they were too conservative in Round 1
- Includes the random “salt” to avoid fault-injection attacks.
- Chooses Vinegar variables randomly instead of deterministically (for side-channel resistance and offline capabilities.)
- Includes a ChaCha8 option

Rainbow Round 2

- Also based on UOV
- First proposed in 2004 with parameters that we too aggressive
- Threads two (or more) UOV instances in a way that improves efficiency but maintains the algebraic complexity
- Introduces new rank-based attack paths, but tunes parameters to account for their complexity

Rainbow map

Fix a finite field $\mathbb{F}_q$. Fix integers

$$0 < v_1 < v_2 < v_3 = n$$

Define $V_i = \{1, \ldots, v_i\}$ & $O_i = \{v_i + 1, \ldots, v_{i+1}\}$.

Set $o_i = |O_i|$. Let l be the index s.t. $k \in O_l$.

$$f^{(k)}(\boldsymbol{x}) = \sum_{i,j \in V_l} \alpha_{ij}^{(k)} x_i x_j + \sum_{i \in V_l, j \in O_l} \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V_l \cup O_l} \gamma_i^{(k)} x_i + \delta^{(k)}$$

Fix T, U, affine maps and construct

$$P(\boldsymbol{x}) = T \circ F \circ U(\boldsymbol{x})$$

Rainbow map Inversion

Algorithm 1 Inversion of the Rainbow central map

Input: Rainbow central map $\mathcal{F} = (f^{(v_1+1)}, \ldots, f^{(n)})$, vector $\mathbf{x} \in \mathbb{F}^m$.

Output: vector $\mathbf{y} \in \mathbb{F}^n$ with $\mathcal{F}(\mathbf{y}) = \mathbf{x}$.

1: Choose random values for the variables $y_1, \ldots, y_{v_1}$ and substitute these values into the polynomials $f^{(i)}$ $(i = v_1 + 1, \ldots, n)$.
2: **for** $\ell = 1$ to u **do**
3: Perform Gaussian Elimination on the polynomials $f^{(i)}$ $(i \in O_\ell)$ to get the values of the variables y_i $(i \in O_\ell)$.
4: Substitute the values of y_i $(i \in O_\ell)$ into the polynomials $f^{(i)}$ $(i = v_{\ell+1} + 1, \ldots, n)$.
5: **end for**
6: **return** $\mathbf{y} = (y_1, \ldots, y_n)$

EUF-CMA Security

- Incorporates a random "salt" in the signature generation process. The public key is inverted at $\mathcal{H}(\mathcal{H}(m \parallel r))$ instead of $\mathcal{H}(m)$.
- With this modification
  - $UUF \Rightarrow EUF - CMA$

Rainbow Setup Parameters

$$\text{Ia} \quad (\mathbb{F}, v_1, o_1, o_2) = (\mathrm{GF}(16), 32, 32, 32) \text{ (64 equations, 96 variables)}$$

$$\text{IIIc} \quad (\mathbb{F}, v_1, o_1, o_2) = (\mathrm{GF}(256), 68, 36, 36) \text{ (72 equations, 140 variables)}$$

$$\text{Vc} \quad (\mathbb{F}, v_1, o_1, o_2) = (\mathrm{GF}(256), 92, 48, 48) \text{ (96 equations, 188 variables)}$$

New Variants

- cyclicRainbow
  - Not actually cyclic, but pseudorandom (not sure why they named it cyclic, exactly.)
  - About 70% smaller keys, but significantly slower verification.
- compressedRainbow
  - Another variant that also pseudorandomly generates a portion of the private key
- We basically asked for these.

Addressing Constant-Timeness

- Use logarithm and exponential tables for multiplication with a large negative log for 0 to achieve constant-time implementations over GF(16).
- For GF(256) they represent elements as degree one polynomials over GF(16) and bootstrap the GF(16) trick.

Constant-Time Gaussian Elimination

- The pivot value is used as a conditional for switching rows and is switched with every row containing a no-zero value.
- Is slower than standard Gaussian elimination by 50% (GF(16)) and 100% (GF(256)).

Rainbow Parameters

parameter set	parameters $(\mathbb{F}, v_1, o_1, o_2)$	public key size (kB)	private key size (kB)	hash size (bit)	signature size (bit) [1]
Ia	(GF(16),32,32,32)	149.0	93.0	256	512
IIIc	(GF(256),68,36,36)	710.6	511.4	576	1,248
Vc	(GF(256), 92,48,48)	1,705.5	1,227.1	768	1,632

[1] 128 bit salt included

cyclic/compressedRainbow Parameters

parameter set	parameters $(\mathbb{F}, v_1, o_1, o_2)$	public key size (kB)	private key size (kB)[2]	hash size (bit)	signature size (bit) [1]
Ia	(GF(16),32,32,32)	58.1	93.0	256	512
IIIc	(GF(256),68,36,36)	206.7	511.4	576	1,248
Vc	(GF(256), 92,48,48)	491.9	1,227.1	768	1,632

[1] 128 bit salt included

[2] can be compressed to a seed of 512 bits (compressed Rainbow)

Rainbow Performance

parameter set		key gen.	sign. gen.	sign. verif.
Ia	cycles	35.0M	402K	155K
	time (ms)	10.6	0.122	0.0468
	memory	3.5MB	3.0MB	2.6MB
IIIc	cycles	340M	1.70M	1.64M
	time (ms)	103	0.516	0.497
	memory	4.6MB	2.9MB	3.1MB
Vc	cycles	757M	3.64M	2.39M
	time (ms)	229	1.10	0.723
	memory	7.0MB	3.7MB	3.9MB

cyclic/compressedRainbow Performance

parameter set		key gen.	sign. gen.*	sign. verif.
Ia	cycles	40.2M	20.2M	3.44M
	time (ms)	12.2	6.13	1.04
	memory	3.5MB	3.0MB	2.6MB
IIIc	cycles	402M	217M	19.4M
	time (ms)	122	65.8	5.89
	memory	4.6MB	2.9MB	3.1MB
Vc	cycles	879M	469M	45.4M
	time (ms)	266	142	13.7
	memory	7.0MB	3.7MB	3.9MB

* decompressing from 512-bit secret key (compressed Rainbow), otherwise same

Security Against Known Attacks

parameter set	parameters $(\mathbb{F}, v_1, o_1, o_2)$	$\log_2$(#gates) direct	MinRank	HighRank	UOV	RBS
Ia	(GF(16),32,32,32)	164.5	161.3	150.3	149.2	**145.0**
		146.5	95.3	**86.3**	87.2	145.0

parameter set	parameters $(\mathbb{F}, v_1, o_1, o_2)$	$\log_2$(#gates) direct	MinRank	HighRank	UOV	RBS
IIIc	(GF(256),68,36,36)	215.2	585.1	313.9	563.8	**217.4**
		183.5	309.1	**169.9**	295.8	217.4

parameter set	parameters $(\mathbb{F}, v_1, o_1, o_2)$	$\log_2$(#gates) direct	MinRank	HighRank	UOV	RBS
Vc	(GF(256),92,48,48)	**275.4**	778.8	411.2	747.4	278.6
		235.5	406.8	**219.2**	393.4	278.6

Changes From Round 1

- Improved Key Generation. Basically the direct analogue of what LUOV does. (Ironic since the argument for this technique provided in Round 1 LUOV comes from the principal submitter of Rainbow which didn't do it in round 1.)
- More focused set of parameters (3 vs. 11ish)
- Cyclic and compressed versions we asked for