Cryptanalysis of ring-LWE based key exchange with key share reuse

ia.cr/2016/085

(paper by Scott Fluhrer)

Tung Chou

Setting

- Ring: $R = \mathbb{Z}[x]/(x^N + 1,\ p)$, $A \in R$
- **Small**: each coefficient follows some narrow distribution D around 0.
- Example: $N = 1024,\ p = 12289,\ D = \Psi_{16}$

Ring-LWE key exchange

Ring-LWE key exchange

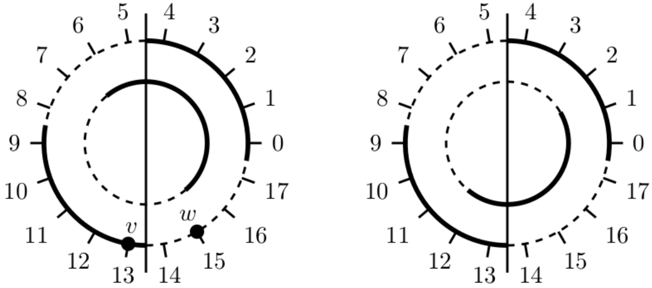
Alice		Bob
	$\xrightarrow{B = AS + E}$	
		$V' \leftarrow BS'$
		$C \leftarrow rec\_gen(V)$
	$\xleftarrow{U = AS' + E', C}$	
$V \leftarrow rec(US, C)$		

Ring-LWE key exchange

Alice		Bob
	$\xrightarrow{B = AS + E}$	
		$V' \leftarrow BS'$
		$C \leftarrow rec\_gen(V)$
	$\xleftarrow{U = AS' + E', C}$	
$V \leftarrow rec(US, C)$		

- $V = ASS' + E'S$
- $V' = ASS' + ES'$

Reconcilation



Picture from “Lattice Cryptography for the Internet” by Chris Peikert, 2014

Attack scenario

- Alice reuses the "key share" $A{\color{blue}S} + {\color{blue}E}$
- Eve's goal is to recover S
- Eve can perform key exchange several times with Alice
- Eve is able to "guess" the shared key for each key exchange

The attack: basis oracle query

- Eve tries to make $(ASS' + E'S)[0] \approx 0$
- Eve sends "$q1 = q2,\ q3 = q4$" instead of "$q1 = q4,\ q2 = q3$" to obtain the sign of $(ASS' + E'S)[0]$
- Even can set $E' = X^{-i}$ and obtain the sign of

$$(ASS' + E'S)[0] = ASS'[0] + S[i]$$

The attack

- Or more generally, $j \cdot \delta + k \cdot s[i]$, where $\delta = ASS'[0]$ (j, k are small; Eve knows the signs of δ and $S[i]$)

- Assume $\delta = \pm 1$. Each $S[i]$ can be derived by setting $k = \delta$ and changing j

- To make sure $\delta = \pm 1$, obtain $S[i]/\delta$ for several i to see the distribution

- $S[i]/\delta$ is obtained by checking the sign of $j\delta + kS[i]$ for several (j, k)'s