Monash University
FIT 5124: Advanced Topics in Security
Week 12 Tutorial Sheet: Revision Questions

Ron Steinfeld, 28 May 2015

This week's tutorial will cover revision questions about the material covered in the whole unit.

1 Problems

1 Explain one type of application scenario where lattice-based cryptography may provide a better solution than classical public-key cryptosystems.

2 Consider the following matrix

$$B = \begin{bmatrix} 4 & 4 & 50 & 12 & 35 \\ 13 & 46 & 30 & 42 & 2 \end{bmatrix}.$$

(a) Suppose this matrix is used in Ajtai's hash function construction with modulus $q = 64$ and input vector $\boldsymbol{x} \in \{0, \ldots, 16\}^5$. What is the hash function H's input and output bit lengths? What is the hash output $H(\boldsymbol{x})$ on input $\boldsymbol{x}^T = [2, 0, 3, 0, 1]$?.

(b) Define the SIS 'perp' lattice $L^{\perp}(B)$ associated with B. Now consider the following two inputs for the above hash function, $\boldsymbol{x}_1^T = [3, 0, 0, 1, 2]$ and $\boldsymbol{x}_2^T = [1, 1, 3, 0, 0]$. Do they form a collision for the hash function H from (a)? If so, explain how to use those inputs to compute a short non-zero vector $\boldsymbol{v}$ in the lattice $L^{\perp}(B)$ and give the value of $\boldsymbol{v}$.

3 Consider the following public-key for Regev's encryption scheme with modulus $q = 32$, $n = 2$, $m = 5$.

$$B^T = \begin{bmatrix} 4 & 4 & 22 & 12 & 29 \\ 13 & 14 & 30 & 17 & 2 \end{bmatrix}, \boldsymbol{y}^T = [24, 21, 10, 11, 26]$$

with secret key $\boldsymbol{s}^T = [2, 1]$.

(a) What is the error vector $\boldsymbol{e}$ used in the key generation?

(b) Explain how to encrypt and decrypt a message bit $b = 1$ with Regev's encryption scheme using the above public key/secret key and the encryption randomness vector $\boldsymbol{r}^T = [-1, 0, -1, 1, 1]$. Does the decryption algorithm return the correct bit? What is the condition on $\boldsymbol{r}$ and $\boldsymbol{e}$ that guarantees correct decryption?

(c) What is the bitlength of the public-key?

(d) How can the length of the public-key be reduced using the Ring-LWE problem?

4 Explain how the LWE problem can be attacked using the LLL algorithm by first reducing LWE to a SIS problem and then applying LLL to the latter. Given that the determinant of the SIS perp lattice for an $m \times n$ LWE matrix A is $q^{n/m}$ and LLL has Hermite Factor γ_{HFLLL}, under what condition will this attack succeed to break LWE?

5 Consider the zero-knowledge EQ protocol in Fig. 5.7 of Lecture 5, which a prover Bob could use to convince a verifier Veronica that Bob knows a secret x such that $g_1^x = h_1$ and $g_2^x = h_2$, where g_1, g_2, h_1, h_2 are public elements in a group G (where the Discrete Log problem is assumed to be hard).

(a) What does the soundness property of this protocol mean, and why does the protocol have this property?

(b) What does the honest verifier ZK property of this protocol mean, and why does the protocol have this property?

(c) Why can't a verifier Veronica use a recorded protocol conversation with prover Bob to convince a third party Alice (who can verify the validity of the protocol response to the protocol challenge) that Veronica communicated with Bob?

6 Consider the 1-of-2 OT protocol in Fig. 7.2 of Lecture 6.

(a) What are the correctness and privacy requirements for this protocol?

(b) Explain why the protocol has the above properties.

(c) Is the protocol secure against a malicious client? Explain why or why not?

7 Explain the principle of cache timing attacks. Give an example of how such an attack might work against an implementation of the AES-128 cryptosystem with a lookup table S-box. Namely, suppose an attacker can inject N chosen input AES plaintexts $x_1, \ldots, x_N$ and measure the corresponding encryption times $t_1, \ldots, t_N$ for some large N. The attacker would like to determing the value of $k_1 \oplus k_2$, where k_1, k_2 are the first two bytes AES key (recall that $z_i = SubBytes(x_i \oplus k_i)$ $(i = 1, \ldots, 16)$ are the S-box output bytes computes in the first round of AES). Explain how the attacker might choose his x_i's and how the attacker may try to estimate the value of $k_1 \oplus k_2$ from the timing measurements. Can the attacker get all bytes of the key by a variation of this technique?

8 Explain the purpose and ideas of the 'Heap engineering' hacking technique for web browser exploitation. Given an example to illustrate your answer.