TTM4135 Worksheet 7: Key Establishment and Post-Quantum Cryptography

Tjerand Silde and Emil August Hovd Olaisen
{tjerand.silde, emil.august.olaisen}@ntnu.no

Spring 2026

1. Review the definitions of the following concepts:
   (a) Key predistribution;
   (b) Session key distribution;
   (c) Key agreement;
   (d) Kerberos;
   (e) Post-quantum cryptography;
   (f) Learning with errors.

2. Discuss the advantages and disadvantages of using key predistribution, session key distribution and key agreement protocols in the following scenarios:
   - a corporate network such as NTNU's Intranet;
   - a small company or domestic environment;
   - Internet communications (e.g. HTTPS, secure email).

3. A potential attack on key establishment protocols is where the attacker makes party A believe that the session key is shared with B but B believes that the same key is shared with C. This is called an *unknown key share attack*.
   - Why might this situation be a serious security problem, even if the attacker does not obtain the key?
   - Why does use of a key derivation function, including the identities of the parties, prevent this attack?

4. There are three main approaches to providing *freshness* (protection against replay of messages) in protocols:
   - random challenges,
   - time stamps, and
   - counters.

   (a) Discuss the advantages and disadvantages of each option.
   (b) The fixed Needham-Schroeder protocol in the lecture uses nonces for freshness. Modify it so that freshness is achieved using counters. Specify the checks that each party must perform on receipt of the protocol messages.

For the following questions we will use $\mathbf{x} \in [\beta]^n$ to denote a column vector with elements bounded by β.

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix},$$

with each element $x_i \in \{-\beta, -\beta+1, \ldots, -1, 0, 1, \ldots, \beta-1, \beta\}$. If we have two column vectors $\mathbf{x}, \mathbf{y}$ of length n we can denote their inner-product as:

$$\mathbf{x}^\intercal \mathbf{y} = \begin{bmatrix} x_1 & x_2 & \ldots & x_n \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \sum_{i=1}^{n} x_i y_i.$$

In the following questions, we will consider vectors over the domain $\mathbb{Z}_q$, we will use coefficients from $[-\lfloor q/4 \rfloor, \ldots, \lfloor 3q/4 \rfloor]$. Here $\lfloor \cdot \rfloor$ denotes rounding down. The bound β will be significantly smaller than q, even smaller than $\lfloor q/4 \rfloor$, we can therefore consider $[\beta]$ as a subset of $\mathbb{Z}_q$.

5. Consider the following toy-encryption scheme:

   - KGen, which will output a short secret key $\mathsf{sk} = \mathbf{s} \leftarrow\!\!\$\ [\beta]^n$ and public key $\mathsf{pk} = (\mathbf{A} \leftarrow\!\!\$\ \mathbb{Z}_q^{n \times n}, \mathbf{t} = \mathbf{A}\mathbf{s})$.
   - $\mathsf{Enc}(\mathsf{pk}, M)$, which on the input of a public key pk and a message $M \in \mathbb{Z}_q$ will sample a random short vector $\mathbf{r} \leftarrow\!\!\$\ [\beta]^n$ and output the ciphertext $c = (\mathbf{u}^\intercal = \mathbf{r}^\intercal \mathbf{A}, v = \mathbf{r}^\intercal \mathbf{t} + M)$.
   - $\mathsf{Dec}(\mathsf{sk}, c)$, which on the input of a secret key sk and ciphertext c will output the message $M' = v - \mathbf{u}^\intercal \mathbf{s}$.

   (a) Show that this scheme is correct, no matter how we choose the parameters n, q, β. That is, show that if $(\mathsf{sk}, \mathsf{pk}) \leftarrow\!\!\$\ \mathsf{KGen}$, then, for all n, q, β:

   $$\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, M)) = M.$$

   (b) Explain why this scheme is insecure (hint: provide an explicit way to conduct a key recovery attack).

6. We define $[\beta]$ as the set of integers in the range $[-\beta, \beta]$. Show that if you have two vectors $\mathbf{x}, \mathbf{y} \in [\beta]^n$, then computing the vector multiplication gives an element bounded by $n\beta^2$. Or in other words, show that $\mathbf{x}^\intercal \mathbf{y} \in [n\beta^2]$.

7. Consider the following encryption scheme:

   - KGen, which will output a secret key $\mathsf{sk} = \mathbf{s} \leftarrow\!\!\$\ [\beta]^n$ and public key $\mathsf{pk} = (\mathbf{A} \leftarrow\!\!\$\ \mathbb{Z}_q^{n \times n}, \mathbf{t} = \mathbf{A}\mathbf{s} + \mathbf{e}_1)$, where the noise value $\mathbf{e}_1 \leftarrow\!\!\$\ [\beta]^n$.
   - $\mathsf{Enc}(\mathsf{pk}, M)$, which on the input of a public key pk and a bit-message $M \in \{0, 1\}$ will sample short random values $\mathbf{r}, \mathbf{e}_2 \leftarrow\!\!\$\ [\beta]^n, e_3 \leftarrow\!\!\$\ [\beta]$ and output the ciphertext $c = (\mathbf{u}^\intercal = \mathbf{r}^\intercal \mathbf{A} + \mathbf{e}_2^\intercal, v = \mathbf{r}^\intercal \mathbf{t} + e_3 + m \cdot \lfloor q/2 \rfloor)$.
   - $\mathsf{Dec}(\mathsf{sk}, c)$, which on the input of a secret key sk and ciphertext c will output $M' = v - \mathbf{u}^\intercal \mathbf{s}$.

   Note that this scheme will not output the same plaintext message, but we will show how to extract it below:

   (a) Why does the attack from task 5 not work on this version of the scheme?

   (b)
   - Show that if $M = 0$ then $M' \in [-\beta(2n\beta + 1), \beta(2n\beta + 1)]$.
   - Show that if $M = 1$ then $M' \in [-\beta(2n\beta + 1) + \lfloor q/2 \rfloor, \beta(2n\beta + 1) + \lfloor q/2 \rfloor]$.

   What this means is that if $M = 0$, then M' will be centered around 0, with each coefficient having a maximum distance of $\beta(2n\beta + 1)$ from 0. If $M = 1$ then each coefficient will be centered around $\lfloor q/2 \rfloor$ with each coefficient having a maximum distance of $\beta(2n\beta + 1)$ from $\lfloor q/2 \rfloor$.

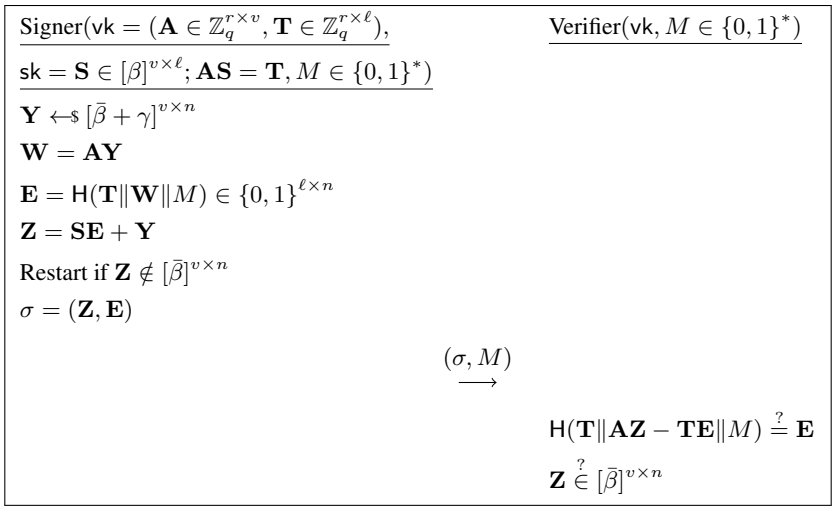

Figure 2: A lattice-based Schnorr-type signature.

(c) Lastly, show that if $4\beta(2n\beta + 1) < q$, then we can always recover M from M'.

8. Consider the lattice-based Schnorr-type digital signature scheme in Figure 2. We use r, v, ℓ, n as dimensions and q as a prime. Let β denote a bound, $\bar{\beta}$ denote a slightly larger bound, $\gamma = \ell \cdot \beta$, and let H be a hash function.

- KGen, which will sample random matrices $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{r\times v}, \mathbf{S} \leftarrow\$ [\beta]^{v\times\ell}$ and compute $\mathbf{AS} = \mathbf{T} \in \mathbb{Z}_q^{r\times\ell}$. The algorithm outputs a public verification key $\mathsf{vk} = (\mathbf{A}, \mathbf{T})$ and a secret signing key $\mathsf{sk} = \mathbf{S}$.
- $\mathsf{Sign}(\mathsf{sk}, M)$, which on the input of a signing key sk and an arbitrary message $M \in \{0,1\}^*$ will repeat the following procedure until success (called a rejection sampling procedure):
  1. Sample a random $\mathbf{Y} \leftarrow\$ [\bar{\beta} + \gamma]^{v\times n}$ and compute $\mathbf{W} = \mathbf{AY}$.
  2. Set $\mathbf{E} = \mathsf{H}(\mathbf{T}\|\mathbf{W}\|M) \in \{0,1\}^{\ell\times n}$ and compute $\mathbf{Z} = \mathbf{SE} + \mathbf{Y}$.
  3. Restart if $\mathbf{Z} \notin [\bar{\beta}]^{v\times n}$.

  Finally, output signature $\sigma = (\mathbf{Z}, \mathbf{E})$ together with the message M.
- $\mathsf{Vf}(\mathsf{vk}, \sigma, M)$, which will output 1 if and only if $\mathsf{H}(\mathbf{T}\|\mathbf{AZ} - \mathbf{TE}\|M) = \mathbf{E}$ and $\mathbf{Z} \in [\bar{\beta}]^{v\times n}$.

(a) Show that the signature scheme is correct. That is, show that if $(\mathsf{vk}, \mathsf{sk}) \leftarrow\$ \mathsf{KGen}$ then:

$$\mathsf{Vf}(\mathsf{vk}, \mathsf{Sign}(\mathsf{sk}, M), M) = 1.$$

(b) Explain why $\mathbf{Z} = \mathbf{SE} + \mathbf{Y}$ is always contained in $[\bar{\beta} + 2\gamma]^{v\times n}$ (before the rejection step). Furthermore, if we assume that $\mathbf{Z}$ is uniformly distributed in $[\bar{\beta} + \gamma]^{v\times n}$, then the probability of success in the rejection sampling step (meaning that $\mathbf{Z} \in [\bar{\beta}]^{v\times n}$) of Sign is:

$$\left(\frac{2\bar{\beta} + 1}{2(\bar{\beta} + 2\gamma) + 1}\right)^{v\cdot n}.$$

How is this success probability of the rejection sampling impacted by the size of $\bar{\beta}$? Why is this rejection sampling step important for efficiency and security?

(c) Consider these two potential adversarial powers:

1. Given the public verification key $\mathsf{vk} = (\mathbf{A}, \mathbf{T})$, find a matrix $\mathbf{S}' \in [\beta]^{v\times\ell}$ such that $\mathbf{AS}' = \mathbf{T}$.
2. Given matrices $\mathbf{W}' \in \mathbb{Z}_q^{r\times n}$ and $\mathbf{E}' \in \{0,1\}^{\ell\times n}$, find $\mathbf{Z}' \in [\bar{\beta}]^{v\times n}$ such that $\mathbf{AZ}' = \mathbf{W}' + \mathbf{TE}'$.

What type of attacks could these adversaries do? Is one of these problems harder than the other? Explain why both of these problems need to be hard for the scheme to be secure.

(d) How does the size of the parameters β and $\bar{\beta}$ impact the hardness of the lattice problems (c)?