NWI-IMC061 – Applied Cryptography

Personalized Appendix, Academic Year 2021–2022

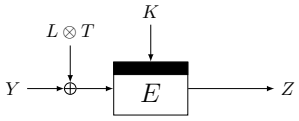
Sequence Number: 8

Appendix to Question 1

Your question will be about PHOTON.
The article can be found at `https://eprint.iacr.org/2011/609.pdf` (skip technicalities of Section 4).

Appendix to Question 2

Consider the following tweakable block cipher $\widetilde{M} : \{0,1\}^{2k} \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, that uses a key $(K, L) \in \{0,1\}^{2k}$ to map a tweak $T \in \{0,1\}^n$ and an input $Y \in \{0,1\}^n$ to a output $Z \in \{0,1\}^n$:



Appendix to Question 3

Consider the following parameters: $b = 1600$, $k = 123$, and $m = 1354$. Consider the following nonce-based authenticated encryption scheme SmaDa (for Small Data), that gets as input a key K of k bits, a nonce N of k bits, and a message M whose length is exactly m bits, and that generates a ciphertext and tag as follows:

$$C \| T = \text{left}_{m+k}(f(K \| N \| 0^m)) \oplus (M \| 0^k)\,,$$

where left_{m+k} returns the leftmost $m+k$ bits of its input (and thus truncates the rightmost k bits in your case).

(The personalized appendix continues on the next page!)

Appendix to Question 4

The encryption cryptosystem is given below.

KeyGen:

1. Choose a random $x \xleftarrow{\$} \mathbb{Z}_q$
2. Choose $\ell = 4$
3. Compute $y \leftarrow g^{25x}$ in G
4. Output public key $\mathsf{pk} = (y, e)$ and private key $\mathsf{sk} = x$ and public parameters (p, ℓ, g)

Encrypt: To encrypt a message M

1. Choose a random $k \xleftarrow{\$} \mathbb{Z}_q$ and
2. Compute ciphertext pair $(C_1, C_2) \leftarrow (g^{k+\ell}, y^k M)$ as

Decrypt: Decrypt ciphertext as $M \leftarrow y^\ell \cdot C_2 \cdot C_1^{-x}$

The remaining parameter used in your personalized version of the assignment is $N = 15$.

Appendix to Question 5

The prover $\mathcal{P}$ is in possession of the secret key $\mathsf{sk} = (s_1, \ldots, s_{14})$. The corresponding public key is $\mathsf{pk} = (P_1, \ldots, P_{14})$, where $P_i = g^{s_i}$ for all $i \in \{1, \ldots, 14\}$.
The protocol $\mathsf{ID}_{\text{Schnorr2}}$ is given below.

$\mathcal{P}(g, \mathsf{sk} = (s_1, \ldots, s_{14}), \mathsf{pk} = (P_1, \ldots, P_{14}))$		$\mathcal{V}(g, \mathsf{pk} = (P_1, \ldots, P_{14}))$
$u \xleftarrow{\$} \mathbb{Z}_q$, $com \leftarrow g^u$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}}$	$\mathsf{ch} \xleftarrow{\$} \mathbb{Z}_{14}$
$\mathsf{resp} \leftarrow u s_{\mathsf{ch}+1}^{-1}$	$\xrightarrow{\mathsf{resp}}$	
		$\mathsf{com} \overset{?}{=} P_{\mathsf{ch}+1}^{\mathsf{resp}}$

The remaining parameter used in your personalized version of the assignment is $\lambda = 256$ and the bit length of q is $\log_2 q = 232$.