Some clarification on security definitions

Ganyu (Bruce) Xu (g66xu)

Spring, 2024

The confusion about what various security definition means seems to be caused by some inconsistencies between the popular textbooks and papers. I consulted two textbooks and found that indeed their security definitions are meaningfully different from what I am familiar with.

1 Textbook definitions

"A graduate course in applied cryptography"[1] introduced the concept of **CPA security** in section 5.3 (page 181):

Definition 1.1 (CPA security from Boneh and Shoup)**.** *For a given cipher $\mathcal{E} = (E, D)$ defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ and for a given adversary $\mathcal{A}$, we define experiments b for $b = 0, 1$:*

1. *The challenge selects $k \xleftarrow{\$} \mathcal{K}$*
2. *The adversary submits a sequence of queries to the challenge. For $i = 1, 2, \ldots$, the i-th query is a pair of messages $m_{i,0}, m_{i,1}$ of the same length. The challenger computes $c_i \leftarrow E(k, m_{i,b})$ and return c_i to the adversary*
3. *The adversary outputs a bit $\hat{b} \in \{0, 1\}$*

Let W_b denote the event that $\mathcal{A}$ outputs 1 in experiment b. We define $\mathcal{A}$'s advantage with respect to $\mathcal{E}$ to be:

$$\text{CPAadv}[A, \mathcal{E}] = |P[W_0] - P[W_1]|$$

A cipher $\mathcal{E}$ is called ***semantically secure against chosen plaintext attack****, or simply* ***CPA secure*** *if for all efficient adversaries,* CPAadv *is negligible.*

"Introduction to modern cryptography"[4] also introduced the concept of CPA security in the context of an adversarial game:

Definition 1.2 (CPA security from Katz and Lindell)**.** *We first define an experiment for any encryption scheme, any adversary, and any value λ for the security parameter:*

1. *A random key is generated*
2. *The adversary is given oracle access to the encryption routine and outputs a pair of messages of the same length*
3. *A random bit is chosen and a ciphertext computed and given to the adversary*
4. *The adversary outputs a bit*
5. *The adversary wins if the output bit is equal to the random bit*

An encryption scheme has ***indistinguishable encryptions under a chosen-plaintext attack****, or is* ***CPA secure****, if for all PPT adversaries there exists a negligible function* negl *such that*

$$P[\hat{b} = b^*] \leq \frac{1}{2} + \text{negl}(\lambda)$$

2 Security definition in research paper

In "A modular analysis of the Fujisaki-Okamoto transformation"[3] by Hofheinz et al, the security definitions are as follows:

Definition 2.1 (OW-ATK)**.** *Let* $\mathrm{PKE} = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ *be a public-key encryption scheme with message space* $\mathcal{M}$*. For* $\mathrm{ATK} \in \{\mathrm{CPA}, \mathrm{PCA}, \mathrm{VA}, \mathrm{PCVA}\}$ *we define OW-ATK game, where*

$$\mathcal{O}_{\mathrm{ATK}} = \begin{cases} - & \mathrm{ATK} = \mathrm{CPA} \\ \mathrm{PCO} & \mathrm{ATK} = \mathrm{CPA} \\ \mathrm{CVO} & \mathrm{ATK} = \mathrm{VA} \\ \mathrm{PCO}, \mathrm{CVO} & \mathrm{ATK} = \mathrm{PCVA} \end{cases}$$

Algorithm 1: OW-ATK game

$(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathrm{Gen}()$;
$m^* \xleftarrow{\$} \mathcal{M}$;
$c^* \leftarrow E(\mathrm{pk}, m^*)$;
$\hat{m} \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{ATK}}}(\mathrm{pk}, c^*)$;
return $[\![\hat{m} = m^*]\!]$

Algorithm 2: $\mathrm{PCO}(m \in \mathcal{M}, c)$

return $[\![D(\mathrm{sk}, c) = m]\!]$

Algorithm 3: $\mathrm{CVO}(c \neq c^*)$

return $[\![D(\mathrm{sk}, c) \in \mathcal{M}]\!]$

3 Conclusion

In the textbooks, "**CPA secure**" really means "**IND-CPA** secure". On the other hand, in research paper, the security definition is always explicitly spelled with both the goal (to break one-wayness or to break indistinguishability) and the adversary's capabilities (access to some specified set of oracles). My guess is that we got confused last week because in public-key cryptography, CPA is a rather meaningless notion because the adversary has the public key, so "one-wayness" automatically implies "one-way security under CPA".

For an example, here is textbook RSA:

Algorithm 4: RSA KeyGen

$p, q \xleftarrow{\$} \mathrm{PrimeGen}()$;
$N \leftarrow p \cdot q$;
$\phi \leftarrow (p-1) \cdot (q-1)$;
$e \leftarrow 3$;
$d \leftarrow e^{-1} \mod \phi$;
return $\mathrm{pk} = (N, e)$, $\mathrm{sk} = d$

Algorithm 5: Encryption $E(\mathrm{pk}, m)$

return $m^e \mod N$

Algorithm 6: Decryption $D(\mathrm{sk}, c)$

return $c^d \mod N$

From the textbooks, **textbook RSA achieves one-wayness but is not CPA secure**, because its encryption is deterministic. On the other hand, using explicit game definitions, we say that RSA is OW-CPA secure but not IND-CPA secure.

OW-CPA and IND-CPA security are commonly accepted standard security notions in. Both Hofheinz[3] and the Kyber team[2] make use of OW-CPA and IND-CPA in their papers. In any case, since I will introduce non-standard security notions, I will explicitly spell out the security games, including the adversary's goal and the adversary's capabilities, so there should be no confusion about the meaning of any terms.

References

[1] Dan Boneh and Victor Shoup. A graduate course in applied cryptography. *Draft 0.5*, 2020.

[2] Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. Crystals-kyber: a cca-secure module-lattice-based kem. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 353–367. IEEE, 2018.

[3] Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. A modular analysis of the fujisaki-okamoto transformation. In *Theory of Cryptography Conference*, pages 341–371. Springer, 2017.

[4] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography: principles and protocols.* Chapman and hall/CRC, 2007.