Faster generic CCA secure KEM transformation using encrypt-then-MAC

Ganyu Xu[1], Guang Gong[1], and Kalikinkar Mandal[2]

[1] University of Waterloo, Waterloo, Ontario, Canada {g66xu,ggong}@uwaterloo.ca
[2] University of New Brunswick, Canada kmandal@unb.ca

Abstract. TODO: write abstract later

Keywords: First keyword · Second keyword · Another keyword.

1 Introduction

Key encapsulation mechanism (KEM) is a public-key cryptographic primitive that allows two parties to establish a shared secret over an insecure communication channel. The accepted security requirement of a KEM is *Indistinguishability under adaptive chosen ciphertext attack (IND-CCA)*. Intuitively speaking, IND-CCA security implies that no efficient adversary (usually defined as probabilistic polynomial time Turing machine) can distinguish a pseudorandom shared secret from a uniformly random bit string of identical length even with access to a decapsulation oracle. Unfortunately, CCA security is difficult to achieve from scratch. Early attempts at constructing CCA secure public-key cryptosystems using only heuristics argument and without using formal proof, such as RSA encryption in PKCS #1 [18] and RSA signature ISO 9796 [1], were badly broken with sophisticated cryptanalysis [8,9,11]. Afterwards, provable chosen ciphertext security became a necessity for new cryptographic protocols. There have been many provable CCA secure constructions since then. Notable examples include Optimal Asymmetric Encryption Padding (OAEP) [7], which is combined with RSA [13] into the widely adopted RSA-OAEP. The Fujisaki-Okamoto transformation [12,14] is another generic CCA secure transformation that was thoroughly studied and widely adopted, particularly by many KEM candidates in NIST's Post Quantum Cryptography (PQC) standardization project.

Chosen ciphertext security is a solved problem within the context of symmetric cryptography. It is well understood that authenticated encryption can be achieved by combining a semantically secure symmetric encryption scheme with an existentially unforgeable message authentication code (MAC) using either the "encrypt-then-MAC" (AES-GCM, ChaCha20-Poly1305) or "MAC-then-encrypt" pattern (AES-CCM)[6,15]. However, adapting this technique for public-key cryptosystems is challenging, since the two communicating parties do not have a pre-shared symmetric key. The first attempt at such adaption is the Diffie-Hellman integrated encryption scheme (DHIES) [3,4] proposed by Abdalla, Bellare, and Rogaway, who proved its chosen ciphertext security under a non-standard but well studied assumption called "Gap Diffie-Hellman problem" [16]. DHIES and its variations appeared in international standards such as IEEE P1363a[2] and ANSI X9.63[5].

1.1 Our contributions

Our contributions are as follows:

Generic CCA secure KEM transformation. We propose the "encrypt-then-MAC" KEM transformation. Our transformation constructs a KEM with provable CCA security under the random oracle model using a public-key encryption scheme with one-wayness under plaintext-checking attack and a message authentication code with existential unforgeability. Compared to the Fujisaki-Okamoto transformation, which is widely adopted by many KEM candidates in NIST's Post Quantum Cryptography (PQC) standardization project, our transformation replaces *de-randomization* (which might degrade the security of a randomized cryptosystem) and *re-encryption* (which is computationally inefficient and introduces additional risk of side channels) with computing MAC tag. We also provided concrete cryptanalysis on possible real-world attacks.

Instantiation with ElGamal and McEliece cryptosystem. We applied our KEM transformation to the ElGamal cryptosystem and the McEliece cryptosystems. We demonstrate that the "encrypt-then-MAC" KEM transformation is a generalization of DHIES by showing that the Gap Diffie-Hellman assumption is a special case of one-way security under plaintext checking attacks. We also surveyed plaintext checking attacks against many post quantum KEM candidates in the PQC standardizaton project.

C implementation of McEliece+. We implemented McEliece+ in C and benchmarked its performance. Compared to the reference implementation of Classic McEliece (which uses re-encryption), McEliece+ achieves significant decapsulation speedup at some minimal cost of encapsulation overhead, which results in 9-12% increase in throughput (encapsulation + decapsulation time).

1.2 Related works

OAEP *Optimal Asymmetric Encryption Padding (OAEP)* [7], proposed by Mihir Bellare and Phillip Rogaway in 1994, was one of the earliest provably secure CCA transformations. However, Victor Shoup identified a non-trivial gap in OAEP's security proof that cannot be filled under ROM[19], although Fujisaki et al. later proved that RSA-OAEP is secure under the RSA assumption [13]. RSA-OAEP is widely used in secure communication protocols such as TLS 1.2. The main drawback of OAEP is that it requires its input to be an one-way trapdoor permutation, which is difficult to find. To this day, RSA remains the only viable candidate to apply OAEP to.

REACT/GEM Okamoto and Pointchval proposed REACT [17] (Figure 1) in 2001, followed by GEM [10] in 2002. Both are generic CCA transformation with security proved under ROM. Okamoto and Pointcheval first defined the security notion of one-wayness under plaintext checking attack (OW-PCA) and reduced the CCA security of the transformation to the OW-PCA security of the input public-key cryptosystem.

$\mathtt{Enc}_{\mathrm{REACT}}(\mathtt{pk}, m)$

$w \leftarrow \mathcal{M}_{\mathtt{PKE}}$
$c_1 \leftarrow \mathtt{Enc}(\mathtt{pk}, w)$
$k \leftarrow G(w)$
$c_2 \leftarrow \mathcal{E}_k(m)$
$c_3 \leftarrow H(w, m, c_1, c_2)$
return (c_1, c_2, c_3)

$\mathtt{Dec}_{\mathrm{REACT}}(\mathtt{sk}, c)$

Require: $(c_1, c_2, c_3) \leftarrow c$
$\hat{w} \leftarrow \mathtt{Dec}(\mathtt{sk}, c_1)$
$\hat{k} \leftarrow G(\hat{w})$
$\hat{m} \leftarrow \mathcal{D}_{\hat{k}}(c_2)$
if $H(\hat{w}, \hat{m}, c_1, c_2) = c_3$ **then**
  return $\hat{m}$
else
  return $\perp$
end if

Fig. 1: Given PKE $(\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$, SKE $(\mathcal{E}, \mathcal{D})$, and hash functions G, H, REACT constructs a hybrid PKE $(\mathtt{Gen}_{\mathrm{REACT}}, \mathtt{Enc}_{\mathrm{REACT}}, \mathtt{Dec}_{\mathrm{REACT}})$

$\mathtt{Enc}_{\mathrm{GEM}}(\mathtt{pk}, m)$

$r \leftarrow \mathcal{R}$
$s \leftarrow F(m, r)$
$w \leftarrow s \| (r \oplus H(s))$
$c_1 \leftarrow \mathtt{Enc}(\mathtt{pk}, w)$
$k \leftarrow G(w, c_1)$
$c_2 \leftarrow \mathcal{E}_k(m)$
return (c_1, c_2)

$\mathtt{Dec}_{\mathrm{GEM}}(\mathtt{sk}, c)$

Require: $(c_1, c_2) \leftarrow c$
$\hat{w} \leftarrow \mathtt{Dec}(\mathtt{sk}, c_1)$
$(\hat{s}, \hat{t}) \leftarrow \hat{w}$
$\hat{r} \leftarrow \hat{t} \oplus H(\hat{s})$
$\hat{k} \leftarrow G(\hat{w}, c_1)$
$\hat{m} \leftarrow \mathcal{D}_{\hat{k}}(c_2)$
if $F(\hat{m}, \hat{r}) = \hat{s}$ **then**
  return $\hat{m}$
else
  return $\perp$
end if

Fig. 2: Given PKE $(\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$, SKE $(\mathcal{E}, \mathcal{D})$, and hash functions F, G, H, GEM constructs a hybrid PKE $(\mathtt{Gen}_{\mathrm{GEM}}, \mathtt{Enc}_{\mathrm{GEM}}, \mathtt{Dec}_{\mathrm{GEM}})$

Fujisaki-Okamoto transformation Fujisaki and Okamoto proposed a generic CCA secure hybrid PKE transformation in 1999

References

1. ISO/IEC 9796: Information Technology — Security Techniques — Digital Signature Scheme Giving Message Recovery, Part 1: Mechanisms Using Redundancy (1999), part 1 of the ISO/IEC 9796 standard
2. Ieee standard specifications for public-key cryptography - amendment 1: Additional techniques. IEEE Std 1363a-2004 (Amendment to IEEE Std 1363-2000) pp. 1–167 (2004). https://doi.org/10.1109/IEEESTD.2004.94612
3. Abdalla, M., Bellare, M., Rogaway, P.: DHAES: an encryption scheme based on the diffie-hellman problem. IACR Cryptol. ePrint Arch. p. 7 (1999), http://eprint.iacr.org/1999/007
4. Abdalla, M., Bellare, M., Rogaway, P.: The oracle diffie-hellman assumptions and an analysis of DHIES. In: Naccache, D. (ed.) Topics in Cryptology - CT-RSA 2001, The Cryptographer's Track at RSA Conference 2001, San Francisco, CA, USA, April 8-12, 2001, Proceedings. Lecture Notes in Computer Science, vol. 2020, pp. 143–158. Springer (2001). https://doi.org/10.1007/3-540-45353-9_12, https://doi.org/10.1007/3-540-45353-9_12
5. ANSI, X.: 63: Public key cryptography for the financial services industry, key agreement and key transport using elliptic curve cryptography. American National Standards Institute (1998)
6. Bellare, M., Namprempre, C.: Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In: Okamoto, T. (ed.) Advances in Cryptology - ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, December 3-7, 2000, Proceedings. Lecture Notes in Computer Science, vol. 1976, pp. 531–545. Springer (2000). https://doi.org/10.1007/3-540-44448-3_41, https://doi.org/10.1007/3-540-44448-3_41
7. Bellare, M., Rogaway, P.: Optimal asymmetric encryption. In: Santis, A.D. (ed.) Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings. Lecture Notes in Computer Science, vol. 950, pp. 92–111. Springer (1994). https://doi.org/10.1007/BFB0053428, https://doi.org/10.1007/BFb0053428
8. Bleichenbacher, D.: Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1. In: Krawczyk, H. (ed.) Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings. Lecture Notes in Computer Science, vol. 1462, pp. 1–12. Springer (1998). https://doi.org/10.1007/BFB0055716, https://doi.org/10.1007/BFb0055716
9. Coppersmith, D., Halevi, S., Jutla, C.: Iso 9796-1 and the new forgery strategy. rump session of Crypto **99** (1999)
10. Coron, J., Handschuh, H., Joye, M., Paillier, P., Pointcheval, D., Tymen, C.: GEM: A generic chosen-ciphertext secure encryption method. In: Preneel, B. (ed.) Topics in Cryptology - CT-RSA 2002, The Cryptographer's Track at the RSA Conference, 2002, San Jose, CA, USA, February 18-22, 2002, Proceedings. Lecture Notes in Computer Science, vol. 2271, pp. 263–276. Springer (2002). https://doi.org/10.1007/3-540-45760-7_18, https://doi.org/10.1007/3-540-45760-7_18

11. Coron, J., Naccache, D., Stern, J.P.: On the security of RSA padding. In: Wiener, M.J. (ed.) Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings. Lecture Notes in Computer Science, vol. 1666, pp. 1–18. Springer (1999). https://doi.org/10.1007/3-540-48405-1_1, https://doi.org/10.1007/3-540-48405-1_1
12. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. In: Wiener, M.J. (ed.) Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings. Lecture Notes in Computer Science, vol. 1666, pp. 537–554. Springer (1999). https://doi.org/10.1007/3-540-48405-1_34, https://doi.org/10.1007/3-540-48405-1_34
13. Fujisaki, E., Okamoto, T., Pointcheval, D., Stern, J.: RSA-OAEP is secure under the RSA assumption. In: Kilian, J. (ed.) Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings. Lecture Notes in Computer Science, vol. 2139, pp. 260–274. Springer (2001). https://doi.org/10.1007/3-540-44647-8_16, https://doi.org/10.1007/3-540-44647-8_16
14. Hofheinz, D., Hövelmanns, K., Kiltz, E.: A modular analysis of the fujisaki-okamoto transformation. In: Kalai, Y., Reyzin, L. (eds.) Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part I. Lecture Notes in Computer Science, vol. 10677, pp. 341–371. Springer (2017). https://doi.org/10.1007/978-3-319-70500-2_12, https://doi.org/10.1007/978-3-319-70500-2_12
15. Krawczyk, H.: The order of encryption and authentication for protecting communications (or: How secure is ssl?). In: Kilian, J. (ed.) Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings. Lecture Notes in Computer Science, vol. 2139, pp. 310–331. Springer (2001). https://doi.org/10.1007/3-540-44647-8_19, https://doi.org/10.1007/3-540-44647-8_19
16. Okamoto, T., Pointcheval, D.: The gap-problems: A new class of problems for the security of cryptographic schemes. In: Kim, K. (ed.) Public Key Cryptography, 4th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2001, Cheju Island, Korea, February 13-15, 2001, Proceedings. Lecture Notes in Computer Science, vol. 1992, pp. 104–118. Springer (2001). https://doi.org/10.1007/3-540-44586-2_8, https://doi.org/10.1007/3-540-44586-2_8
17. Okamoto, T., Pointcheval, D.: REACT: rapid enhanced-security asymmetric cryptosystem transform. In: Naccache, D. (ed.) Topics in Cryptology - CT-RSA 2001, The Cryptographer's Track at RSA Conference 2001, San Francisco, CA, USA, April 8-12, 2001, Proceedings. Lecture Notes in Computer Science, vol. 2020, pp. 159–175. Springer (2001). https://doi.org/10.1007/3-540-45353-9_13, https://doi.org/10.1007/3-540-45353-9_13
18. RSA Data Security, I.: PKCS 1: RSA Encryption Standard Version 1.5. Request for Comments: 2313 (Mar 1998), https://www.rfc-editor.org/rfc/rfc2313
19. Shoup, V.: OAEP reconsidered. In: Kilian, J. (ed.) Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings. Lecture Notes in Computer Science, vol. 2139, pp. 239–259. Springer (2001). https://doi.org/10.1007/3-540-44647-8_15, https://doi.org/10.1007/3-540-44647-8_15