2E-1

On the Security of Proxy Re-Encryption Schemes

Kousuke Nagumo
Department of Mathematical and Computing Sciences,
Tokyo Institute of Technology

Keisuke Tanaka
Department of Mathematical and Computing Sciences,
Tokyo Institute of Technology

In PKC 2010, Matsuda, Nishimaki and Tanaka proposed a bidirectional proxy re-encryption (PRE) scheme from a recently cryptographic primitive named reapplicable loosy trapdoor functions [2] , and claimed that their scheme is chosen ciphertext secure without bilinear maps in the standard model [1] . However, the gap in the security proof and the attack of this scheme was announced by Jian Weng and Yunlei Zhao in the eprint archive [3]. In their paper, they indicated that the Matsuda-Nishimaki-Tanaka PRE scheme fails to achieve the chosen-ciphertext security. But, it does not mean that all of the instantiations of the abstract scheme is insecure. In this paper we analize their attack and describe when it works. We also discuss the possibility on the secure construction for bidirectional proxy re-encryption schemes.

The Matuda-Nishimaki-Tanaka PRE Scheme

Proxy re-encryption was created by Blaze et al. in Eurocrypt'98. This technique achieves a semi-trust proxy to translate a ciphertext related to Alice into another ciphertext related to Bob. The proxy cannot obtain the information about the underlying messages. Blaze et al. suggested the bidirectional PRE scheme, and Ateniese et al. presented unidirectional PRE schemes by using bilinear maps. These techniques are secure only against the chosen plaintext attack (CPA). But, in general, applications require security against the chosen ciphertext attack (CCA). Regarding this problem, Canetti and Hohenberger suggested the first CCA-secure bidirectional multi-hop PRE scheme in the standard model. Many researchers created techniques for constructing the schems secure against the chosen ciphertext attack. These schemes are based on bilinear maps. Canetti and Hohenber mentioned an open problem of constructing CCA-secure PRE schemes without bilinear maps. In PKC 2010, Matsuda, Nishimaki and Tanaka suggested a bidirectional proxy reencryption scheme without using bilinear maps. This scheme claimed that their scheme is CCA-secure in the standarad model. However, the gap in the security proof and the attack of this scheme was announced by Jian Weng and Yunlei Zhao in the eprint archive.

The Attack by Weng and Zhao

We review a concrete CCA-attack against the Matsuda-Nishimaki-Tanaka PRE scheme [3] by Weng and Yunlei. Before presenting the attack, we would like mention a fundamental principle for designing CCA-secure PRE schemes, i.e., the validity of all the ciphertext components in the original ciphertext should be able to be veri-

fied by the *proxy*. Unfortunately, the Matsuda-Nishimaki-Tanaka PRE scheme violates this principle. Indeed, for a ciphertext $C_i = (vk, c_{1,i}, c_2, c_3, \tau, \sigma)$, the validity of vk, c_2, c_3, τ and σ can be ensured by checking whether $\mathbf{SigVer}(vk, (c_2, c_3, \tau'), \sigma) = 1$ holds. However, it is impossible for the proxy to verify the validity of component $c_{1,i}$: observe that in the encryption algorithm, component $c_{1,i}$ is not included in the generation of the one-time signature, and it will be transformed into $c_{1,j}$ in the re-encryption algorithm. Thus, the Matsuda-Nishimaki-Tanaka PRE scheme inevitably suffers from a chosen-ciphertext attack. Roughly speaking, an adversary can break the CCA-security of the Matsuda-Nishimaki- Tanaka PRE scheme as follows: Given the challenge ciphertext $C_{i^*} = (vk, c_{1,i^*}, c_2, c_3, \tau, \sigma)$, the adversary can first modify the ciphertext component c_{1,i^*} to obtain a new (ill-formed) ciphertext C'_{i^*} and then ask the re-encryption oracle to re-encrypt C'_{i^*} into another ciphertext C'_j for a *corrupted* user j (note that according to the security model, it is legal for the adversary to issue such a query); next, the adversary can modify C'_j to obtain the *right* reencrypted ciphertext C_j of the challenge ciphertext, and thus he can obtain the underlying plaintext by decrypting C_j with user $j's$ secret key.

References

[1] Matsuda, T., Nishimaki, R., and Tanaka, K. CCA Proxy Re-Encryption without Bilinear Maps in the Standard Model. In *Public Key Cryptography* (2010), P. Q. Nguyen and D. Pointcheval, Eds., vol. 6056 of *Lecture Notes in Computer Science*, Springer, pp. 261–278.

[2] Peikert, C., and Waters, B. Lossy trapdoor functions and their applications. In *STOC* (2008), C. Dwork, Ed., ACM, pp. 187–196.

[3] Weng, J., and Zhao, Y. On the security of a bidirectional proxy re-encryption scheme from pkc 2010. *eprint* (2010).