SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Lossy Trapdoor function の幾つかの亜種について
On some variants of lossy trapdoor function

星野 文学 *
Fumitaka Hoshino

キーワード Lossy Trapdoor function, Dual Projective Hashing, Universal Projective Hashing, Lossy Trapdoor Relation

あらまし

$\lambda \in \mathbb{N}$ をセキュリティパラメタとすると lossy trapdoor function とは次の確率的多項式時間アルゴリズムの組 $(\mathtt{Gen}, \mathtt{Eval}, \mathtt{Invert})$ である.

$$\mathtt{Gen} : 1^\lambda, b \xmapsto{\$} (s,t) \text{ where } t = \perp \text{ if } b = 1.$$

$$\mathtt{Eval} : s, x \xmapsto{\$} f_s(x) \text{ where } f_s \text{ is injective if } b = 0, \text{ and lossy if } b = 1.$$

$$\mathtt{Invert} : t, f_s(x) \xmapsto{\$} x \text{ if } b = 0.$$

ここで, 関数 f_s の定義域を X とすると, $b = 0$ のとき $|f_s(X)|/|X| = 1$ (即ち単射) $b = 1$ のとき $|f_s(X)|/|X| \sim O(2^{-\lambda})$ でかつ $\{s|(s,t) \leftarrow \mathtt{Gen}(1^\lambda, 0)\}$ の分布と $\{s|(s,t) \leftarrow \mathtt{Gen}(1^\lambda, 1)\}$ の分布が λ に関して計算量的に識別不能とする. Peikert と Waters は STOC 2008 において lossy trapdoor function の概念を提唱し, その具体的構成と応用を提案した [1–3]. その後 lossy trapdoor function の構成法や拡張および応用などに関して様々な研究が行われている [4–8]. 本発表では Lossy Trapdoor function の幾つかの亜種について考察を行う.

参考文献

[1] C. Peikert and B. Waters, "Lossy trapdoor functions and their applications," IACR Cryptol. ePrint Arch., p.279, 2007. URL: http://eprint.iacr.org/2007/279.

[2] C. Peikert and B. Waters, "Lossy trapdoor functions and their applications," Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008, ed. C. Dwork, pp.187–196, ACM, 2008. doi:10.1145/1374376.1374406.

[3] C. Peikert and B. Waters, "Lossy trapdoor functions and their applications," SIAM J. Comput., vol.40, no.6, pp.1803–1844, 2011. doi:10.1137/080733954.

[4] B. Hemenway and R. Ostrovsky, "Building lossy trapdoor functions from lossy encryption," Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part II, ed. K. Sako and P. Sarkar, Lecture Notes in Computer Science, vol.8270, pp.241–260, Springer, 2013. doi:10.1007/978-3-642-42045-0_13.

[5] B. Hemenway and R. Ostrovsky, "Building lossy trapdoor functions from lossy encryption," IACR Cryptol. ePrint Arch., p.156, 2015. URL: http://eprint.iacr.org/2015/156.

[6] H. Xue, X. Lu, B. Li, and Y. Liu, "Lossy trapdoor relation and its applications to lossy encryption and adaptive trapdoor relation," Provable Security - 8th International Conference, ProvSec 2014, Hong Kong, China, October 9-10, 2014. Proceedings, ed. S.S.M. Chow, J.K. Liu, L.C.K. Hui, and S. Yiu, Lecture Notes in Computer Science, vol.8782, pp.162–177, Springer, 2014. doi:10.1007/978-3-319-12475-9_12.

[7] H. Xue, Y. Liu, X. Lu, and B. Li, "Lossy projective hashing and its applications," Progress in Cryptology - INDOCRYPT 2015 - 16th International Conference on Cryptology in India, Bangalore, India, December 6-9, 2015, Proceedings, ed. A. Biryukov and V. Goyal, Lecture Notes in Computer Science, vol.9462, pp.64–84, Springer, 2015. doi:10.1007/978-3-319-26617-6_4.

[8] Z. Zhang, Y. Chen, S.S.M. Chow, G. Hanaoka, Z. Cao, and Y. Zhao, "All-but-one dual projective hashing and its applications," Applied Cryptography and Network Security - 12th International Conference, ACNS 2014, Lausanne, Switzerland, June 10-13, 2014. Proceedings, ed. I. Boureanu, P. Owesarski, and S. Vaudenay, Lecture Notes in Computer Science, vol.8479, pp.181–198, Springer, 2014. doi:10.1007/978-3-319-07536-5_12.

[9] R. Cramer and V. Shoup, "Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption," Advances in Cryptology—EUROCRYPTO 2002, ed. L. Knudsen, LNCS, vol.2332, pp.45–64, Springer-Verlag, 2002.

* 長崎県立大学, 〒851-2195 長崎県西彼杵郡長与町まなび野 1-1-1, University of Nagasaki, 1-1-1 Manabino, Nagayo-cho, Nishi-Sonogi-gun, Nagasaki 851-2195, JAPAN, hoshino@sun.ac.jp