МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 1 С. 13–30

УДК 519.719.2+519.712

Схема разделения секрета типа схемы Блэкли, основанная на пересечении подпространств

Ю. В. Косолапов

Южный федеральный университет, Ростов-на-Дону

Получено 23.V.2016

Аннотация. Рассматривается задача построения схемы разделения секрета, в которой возможна замена любого подмножества участников новыми участниками; при этом доли секрета вычисляются только для новых участников, а доли секрета у незамененных участников остаются прежними. С помощью теории помехоустойчивых кодов строятся протоколы разделения и восстановления секрета. Для исследования допустимых границ параметров построенной схемы распределения секрета вводится и исследуется новая характеристика линейного кода. В качестве примеров приводятся реализации предложенной схемы на основе некоторых кодов.

Ключевые слова: схема разделения секрета, пересечение подпространств, линейный код

Blakley type secret sharing scheme based on the intersection of subspaces

Yu. V. Kosolapov

Southern Federal University, Rostov-on-Don

Abstract. We consider the problem of constructing a secret sharing schemes permitting to replace any subset of participants with new participants so that new secret shares may be calculated only for the newly added members, and secret shares of others participants do not change. Using the theory of error-correcting codes we construct protocols of separation and recovery of the secret. In order to study the permissible domains of parameters of this secret sharing scheme the new characteristics of linear code is introduced and explored. We implement the proposed scheme for some linear codes as examples.

Key words: secret sharing scheme, subspace intersection, linear code
Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 1, pp. 13–30 (Russian)

Список литературы

[1] Cramer R., Damgard I., Maurer U., "General secure multi-party computation from any linear secret-sharing scheme". In: "*EUROCRYPT 2000*", Lect. Notes Comput. Sci., **1807**, 2000, 316–334.

[2] Chen H., Cramer R., Goldwasser S., Haan R., Vaikuntanathan V., "Secure computation from random error correcting codes". In: "*EUROCRYPT 2007*", Lect. Notes Comput. Sci., **4515**, 2007, 291–310.

[3] Погорелов Б. А., Сачков В. Н., *Словарь криптографических терминов*, М. : МЦНМО, 2006, 91 с.

[4] Shamir A., "How to share a secret", *Comm. ACM*, **22**:11 (1979), 612–613.

[5] Blakley G. R., "Safeguarding cryptographic keys". In: "*AFIPS Conf. Proc.*", **48**, 1979, 313–317..

[6] Brickell E. F., "Some ideal secret sharing schemes". In: "*EUROCRYPT'89*", Lect. Notes Comput. Sci., **434**, 1989, 468–475.

[7] Blakley G. R., Kabatianski G A., "Linear algebra approach to secret sharing schemes". In: "*Error Control, Cryptology, and Speech Compression*", Lect. Notes Comput. Sci., **829**, 1994, 33–40..

[8] Dijk M., "A linear construction of perfect secret sharing schemes". In: "*EUROCRYPT'94*", Lect. Notes Comput. Sci., **950**, 1994, 23–34.

[9] Ozarov L. H., Wyner A. D., "Wire-tap channel II", *Bell Labs Techn. J.*, **63**:10 (1984), 2135–2157..

[10] Деундяк В. М., Косолапов Ю. В., "Об одном методе снятия неопределенности в канале с помехами в случае применения кодового зашумления", *Изв. ЮФУ. Техн. науки* (2014), 197–208.

[11] Sendrier N., "Finding the permutation between equivalent linear codes: the support splitting algorithm", *IEEE Trans. Inf. Theory*, **46**:4 (2000), 1193–1203.

[12] Forney G. D., "Dimension/length profiles and Trellis complexity of linear block codes", *IEEE Trans. Inf. Theory*, **40**:6 (1994), 1741–1752.

[13] Деундяк В. М., Маевский А. Э., Могилевская Н. С., *Методы помехоустойчивой защиты данных*, Ростов-н/Д : ЮФУ, 2014, 308 с.

[14] Wei V. K., "Generalized Hamming weights for linear codes", *IEEE Trans. Inf. Theory*, **37**:5 (1991), 1412–1418.

[15] Dodunekov S. M., Landgev I. N., "On near-MDS codes". In: "*Proc. IEEE Int. Symp. Inf. Theory*", 1994, 427.

[16] Chabot C., "Recognition of a code in a noisy environment". In: "*Proc. IEEE Int. Symp. Inf. Theory*", 2007, 2211–2215.

[17] Ding P., Key J. D., "Minimum-weight codewords as generators of generalized Reed – Muller codes", *IEEE Trans. Inf. Theory*, **46**:6 (2000), 2152–2157.

[18] Blake I. F., Mullin R. C., *The Mathematical Theory of Coding*, N. Y. : Academic Press, 1975, 368 pp.

[19] Косолапов Ю. В., "Верхняя граница иерархии весов регулярных слабоплотных кодов специального вида", *Интегро-дифф. операторы и их прил. Межвуз. сб. науч. тр.*, № 8 (2008), 72–80.

[20] Барг С., "Некоторые новые NP-полные задачи кодирования", *Проблемы передачи информации*, **30**:3 (1994), 23–28.

[21] Bouyukliev I., Bakoev V., "A method for efficiently computing the number of codewords of fixed weights in linear codes", *Discr. Appl. Math.*, **156**:15 (2008), 2986–3004.

[22] Зубков А. М., Круглов В. И., “Статистические характеристики весовых спектров случайных линейных кодов на $\mathrm{GF}(p)$ ”, *Математические вопросы криптографии*, **5**:1 (2014), 27–38.