UDC 517.9

On the Construction of (n, k)-schemes of Visual Cryptography Using a Class of Linear Hash Functions Over a Binary Field

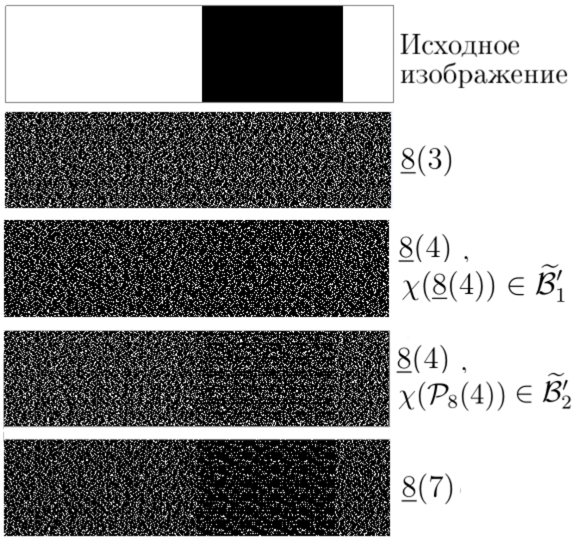
Yu. V. Kosolapov

Yury V. Kosolapov, https://orcid.org/0000-0002-1491-524X, Southern Federal University, 105/42, Bol'shaya Sadovaya Str., Rostov-on-Don, 344006, Russia, itaim@mail.ru

The paper explores the use of a set of hash functions for constructing a secret sharing scheme among n participants based on the (k, k)-scheme M. Nahor and A. Shamir. Conditions are obtained for a set of hash functions, in which it is possible to construct (k, n)-schemes where any coalition of power k or more can restore a secret, and a coalition of lower power cannot restore the secret. In particular, the application of the class of linear hash functions is investigated. In general, this class does not allow us to construct a (k, n)-scheme, but it is possible to construct a (k, K, n)-scheme for which any $k - 1$ and less participants cannot restore the secret, and any K and more can. For a class of linear hash functions, sufficient conditions are obtained for K, in which the coalition of power K and more can restore the secret. In a particular case, a secret sharing scheme for eight participants was developed, based on the $(4, 4)$-scheme of M. Naor and A. Shamir using a class of linear hash functions. It is shown that for any 4-power coalition the secret can be restored, that is, the constructed scheme is a $(8, 4)$-scheme. The $(8, 4)$-scheme constructed in particular is characterized by a shorter length of shares than the $(8, 4)$-scheme constructed in accordance with the algorithm proposed by M. Naor and A. Shamir.

Key words: secret sharing scheme, visual cryptography, linear hash functions.

DOI: 10.18500/1816-9791-2018-18-2-227-239



Applications of $(8, 4)$-scheme

Таблица 1 / Table 1

Распределение $C(b_3(B), f_{h(H)})$ для $\widetilde{\mathscr{B}}_{3,1}$ и $\mathscr{H}_2$

The distribution of $C(b_3(B), f_{h(H)})$ for $\mathscr{B}_{3,1}$ and $\mathscr{H}_2$

Матрица / Matrix	$\mathscr{H}_{2,1}$		$\mathscr{H}_{2,2}$		$\mathscr{H}_{2,3}$	
$C(b_3(B), f_{h(H)})$	*3*	*4*	*3*	*4*	*3*	*4*
$B \in \widetilde{\mathscr{B}}_{3,1}$	18	0	18	0	0	6

Таблица 2 / Table 2

Распределение $C(b_3(B), f_{h(H)})$ для $\widetilde{\mathscr{B}}_{3,2}$ и $\mathscr{H}_2$

The distribution of $C(b_3(B), f_{h(H)})$ for $\mathscr{B}_{3,2}$ and $\mathscr{H}_2$

<table>
<tr><td>Матрица / Matrix</td><td colspan="2">$\mathscr{H}_{2,1}$</td><td colspan="2">$\mathscr{H}_{2,2}$</td><td colspan="2">$\mathscr{H}_{2,3}$</td></tr>
<tr><td>$C(b_3(B), f_{h(H)})$</td><td>2</td><td>4</td><td>2</td><td>4</td><td>2</td><td>4</td></tr>
<tr><td>B_2, B_3, B_4</td><td>6</td><td>12</td><td rowspan="2">6</td><td rowspan="2">12</td><td>6</td><td>0</td></tr>
<tr><td>B_5, B_6, B_7</td><td>12</td><td>6</td><td rowspan="2">0</td><td rowspan="2">6</td></tr>
<tr><td>B_1</td><td>0</td><td>18</td><td>18</td><td>0</td></tr>
</table>

Таблица 3 / Table 3

Распределение $C(b_3(B), f_{h(H)})$ для $\widetilde{\mathscr{B}}_{3,3}$ и $\mathscr{H}_2$

The distribution of $C(b_3(B), f_{h(H)})$ for $\mathscr{B}_{3,3}$ and $\mathscr{H}_2$

Матрица / Matrix	$\mathscr{H}_{2,1}$		$\mathscr{H}_{2,2}$		$\mathscr{H}_{2,3}$	
$C(b_3(B), f_{h(H)})$	3	4	3	4	3	4
$B \in \widetilde{\mathscr{B}}_{3,3}$	12	6	18	0	6	0

Таблица 4 / Table 4

Распределение $C(b_3(B), f_{h(H)})$ для $\widetilde{\mathscr{B}}_2$ и $\mathscr{H}_1$

The distribution of $C(b_3(B), f_{h(H)})$ for $\mathscr{B}_2$ and $\mathscr{H}_1$

Матрица / Matrix	$\mathscr{H}_{1,1}$		$\mathscr{H}_{1,2}$		$\mathscr{H}_{1,3}$	
$C(b_3(B), f_{h(H)})$	1	2	1	2	1	2
$\widehat{B}_4$	3	0	0	9	0	9
$\widehat{B}_1, \widehat{B}_2, \widehat{B}_3$	0	3	0	9	3	6
$\widehat{B}_5, \widehat{B}_6, \widehat{B}_7$	0	3	3	6	0	9

References

1. Shamir A. How to share a secret. *Communications of the ACM*, 1979, vol. 22, № 11, pp. 612–613.
2. Blakley G. R. Safeguarding cryptographic keys. *Proc. of the National Computer Conference*, 1979, vol. 48, pp. 313–317.
3. Pogorelov B. A., Sachkov V. N. *Slovar' kriptograficheskih terminov* [Dictionary of cryptographic terms]. Moscow, MTsNMO, 2006. 91 p.(in Russian).
4. Chen H., Cramer R., Goldwasser S., Haan R., Vaikuntanathan V. Secure Computation from Random Error Correcting Codes. *Advances in Cryptology – EUROCRYPT 2007. EUROCRYPT 2007. Lecture Notes in Computer Science*. Berlin, Heidelberg, Springer, 2007, vol. 4515, pp. 291–310. DOI: 10.1007/978-3-540-72540-4_17
5. Naor M., Shamir A. Visual cryptography. *Advances in Cryptology — EUROCRYPT'94. EUROCRYPT 1994. Lecture Notes in Computer Science*. Berlin, Heidelberg, Springer, 1994, vol. 950, pp. 1–12. DOI: 10.1007/BFb0053419
6. Pelli D.G., Bex P. Measuring contrast sensitivity. *Vision Res.*, 2013, vol. 90, pp. 10–14. DOI: 10.1016/j.visres.2013.04.015
7. Carter J. L., Wegman M. N. Universal classes of hash functions. *Journal of Computer and System Sciences*, 1979, vol. 18, iss. 2, pp. 143–154. DOI: 10.1016/0022-0000(79)90044-8
8. Bose M., Mukerjee R. Optimal (k, n) visual cryptographic schemes for general k. *Des. Codes Cryptogr.*, 2010, vol. 55, iss. 1, pp. 19–35. DOI: 10.1007/s10623-009-9327-6
9. Cormen T. H., Leiserson C. E., Rivest R. L., Stein C. *Introduction to Algorithms*. Cambridge, Massachusetts; London, England, MIT Press, 2009. 1312 p.
10. Lakshmanan R., Arumugam S. Construction of a (k, n)-visual cryptography scheme. *Des. Codes Cryptogr.*, 2017, vol. 82, iss. 3, pp. 629–645. DOI: 10.1007/s10623-016-0181-z

Cite this article as:
Kosolapov Yu. V. On the Construction of (k, n)-Schemes of Visual Cryptography Using a Class of Linear Hash Functions Over a Binary Field. *Izv. Saratov Univ. (N. S.), Ser. Math. Mech. Inform.*, 2018, vol. 18, iss. 2, pp. 227–239 (in Russian). DOI: 10.18500/1816-9791-2018-18-2-227-239.