

# Corrections to “Secret sharing schemes with bipartite access structure” \*

Carles Padró, Germán Sáez

Dept. Matemàtica Aplicada IV, Universitat Politècnica de Catalunya  
C. Jordi Girona, 1-3, Mòdul C3, Campus Nord, 08034 Barcelona, Spain  
e-mail: {matcpl,german}@mat.upc.es

We point out some mistakes in Lemma 5.1 and Proposition 5.2 in our paper.

Since we are supposing that  $a \leq b$ , the first and the second statements of Lemma 5.1 are not symmetric. The second one must be corrected to:

$$2. \ y_r = \max\{0, \lceil (t - aN_1)/b \rceil\} \text{ and } x_r = \lceil (t - by_r)/a \rceil.$$

Besides, the proof of Lemma 5.1 can be more easily understood by beginning it with the proof of the third statement.

Due to this mistake in Lemma 5.1, the statement and the proof of Proposition 5.2 are not correct. Proposition 5.2, which is a characterization of the ideal weighted threshold access structures with two weights, must be changed to:

**Proposition 5.2** *A weighted threshold access structure with two weights  $\Gamma = W(a, b, t, N_1, N_2)$  is ideal if and only if one of the following situations occurs:*

- $x_1 + y_1 = x_r + y_r$ , where  $x_1 = 0$  or  $y_1 = N_2$ , that is,  $\Gamma = \Omega_4(n, n_1, n_2)$  with  $n_1 = x_r$ ,  $n_2 = y_1$  and  $n = x_1 + y_1$ .
- $r = 2$  and  $x_1 = 0$ , that is,  $\Gamma = \Omega_2(n, n_1, n_2)$ , where  $n_1 = x_2$ ,  $n_2 = y_1$  and  $n = x_2 + y_2$ .
- $r \geq 3$ ,  $x_1 = 0$ ,  $x_2 = 2$  and  $x_2 + y_2 = x_r + y_r$ , that is,  $\Gamma = \Omega_2(n, n_1, n_2)$ , where  $n_1 = x_r$ ,  $n_2 = y_1$  and  $n = n_2 + 2$ .

---

\*C. Padró and G. Sáez, *IEEE Trans. Inform. Theory*, vol. 46, pp. 2596–2604, Nov. 2000.

The proof must be corrected by taking into account that the first situation does not imply that  $\Gamma$  is a threshold structure.

Finally, we point out that Conjecture 6.1 is false. According to the results in [1], the access structures related to the non-Pappus matroid are not vector space access structures but they can be realized by an ideal secret sharing scheme. Therefore, they are counterexamples to our conjecture.

## Acknowledgments

We thank Michael J. Collins, who noticed the mistakes in the statements of Lemma 5.1 and Proposition 5.2.

## References

- [1] J. Simonis, A. Ashikhmin, “Almost affine codes,” *Des. Codes Cryptogr.*, vol. 14, pp. 179–197, May 1998.