Properties of distinct-difference configurations and lightweight key predistribution schemes for grid-based networks

Simon R. Blackburn[1] Keith M. Martin[1] Tuvi Etzion[2]
Maura B. Paterson[1]

[1]Information Security Group
Royal Holloway, University of London

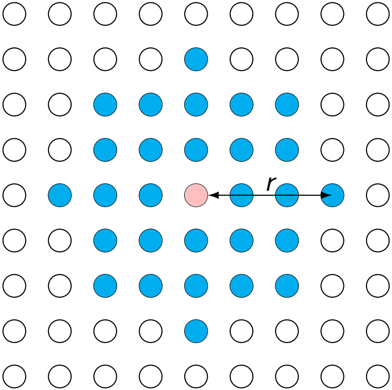
[2]Technion -Israel Institute of Technology
Department of Computer Science

19 May 2009

Outline

Precision Agriculture

Grid-Based Wireless Sensor Networks

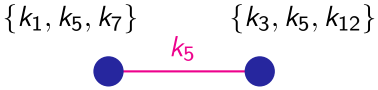


- restricted memory
- restricted battery power
- restricted computational ability
- vulnerable to compromise

Key Predistribution

Definition (key predistribution scheme (KPS))

- nodes are assigned keys before deployment
- nodes that share keys can communicate securely



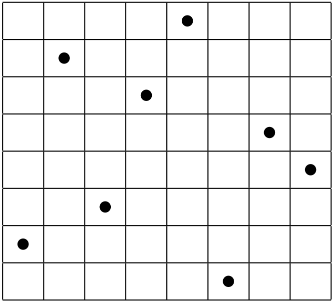
e.g. Eschenauer and Gligor: Each node randomly draws m keys uniformly without replacement from a keypool $\mathcal{K}$

Goals for a KPS in a Grid-Based Network

- enable as many pairs of neighbouring nodes as possible to communicate securely
- minimise storage
- be resilient against node compromise

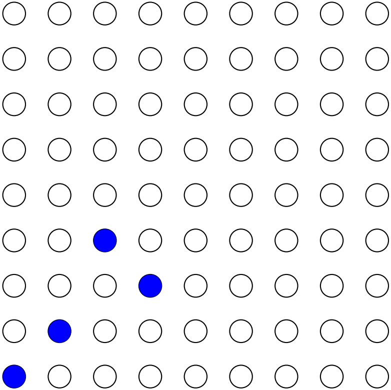
Observation: it is not necessary for two nodes to share more than one key

Costas Arrays

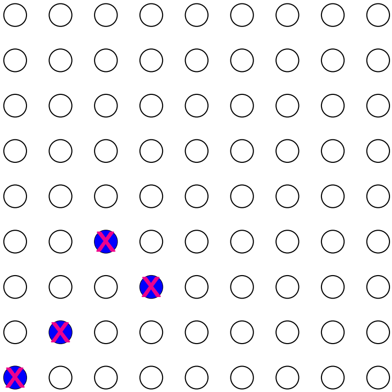


- one dot per row/column
- vector differences between dots are distinct
- applications to sonar, radar
- known constructions are based on finite fields

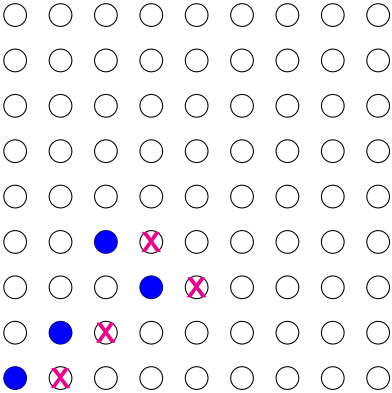
Translated Costas Arrays Overlap in at Most One Point



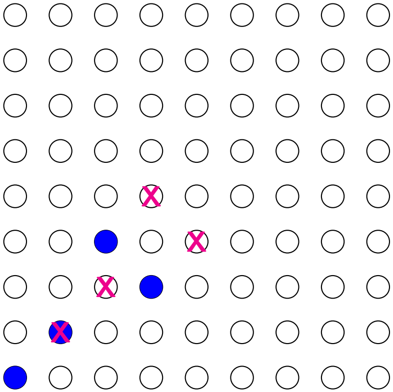
Translated Costas Arrays Overlap in at Most One Point



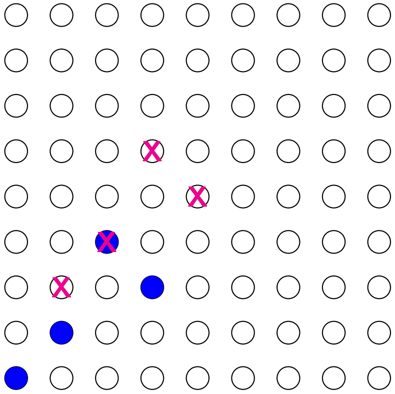
Translated Costas Arrays Overlap in at Most One Point



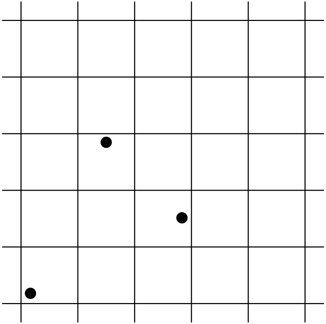
Translated Costas Arrays Overlap in at Most One Point



Translated Costas Arrays Overlap in at Most One Point

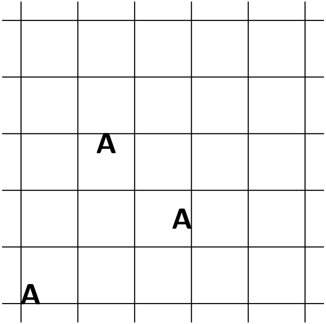


Key Predistribution Using Costas Arrays



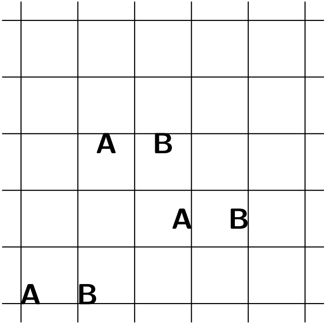
- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$

Key Predistribution Using Costas Arrays



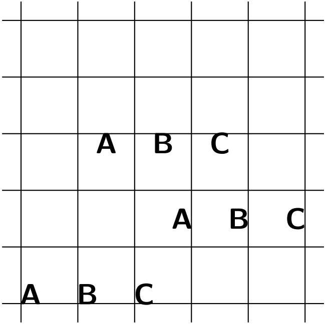
- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$

Key Predistribution Using Costas Arrays



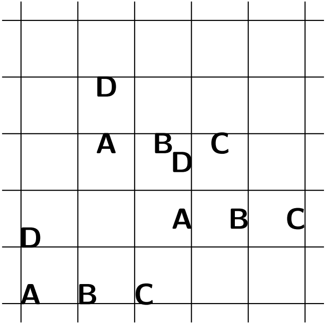
- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$

Key Predistribution Using Costas Arrays



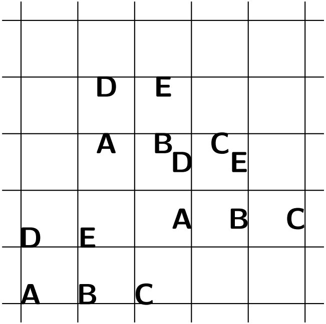
- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$

Key Predistribution Using Costas Arrays



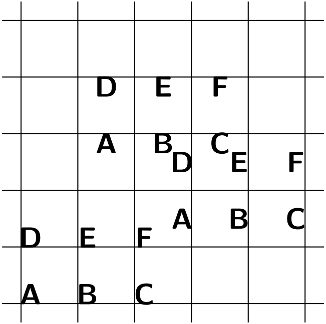
- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$

Key Predistribution Using Costas Arrays



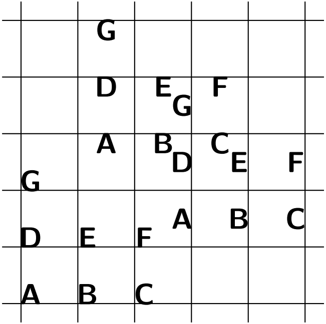
- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$

Key Predistribution Using Costas Arrays



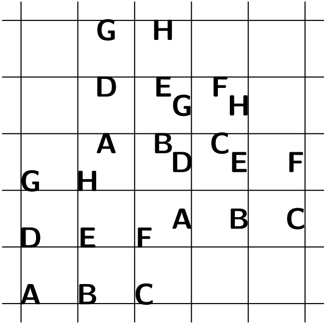
- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$

Key Predistribution Using Costas Arrays



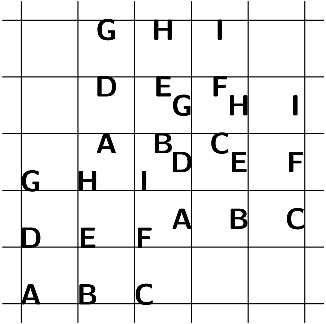
- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$

Key Predistribution Using Costas Arrays



- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$

Key Predistribution Using Costas Arrays

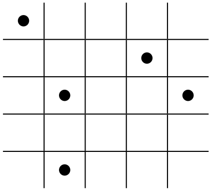


- uses an $n \times n$ Costas array
- each sensor stores n keys
- each key is assigned to n sensors
- two sensors share at most one key
- the distance between two sensors that share a key is at most $\sqrt{2}(n-1)$

Distinct-Difference Configurations

Definition (Distinct-Difference Configuration DD(m, r))

- m dots are placed in a square grid
- the distance between any two dots is at most r
- vector differences between dots are all distinct



DD$(5, 8)$

- can be used for key predistribution in the same way as a Costas array
- more general than a Costas array $\Rightarrow$ more flexible choice of parameters

Upper Bounds on m

Theorem

If a $\mathrm{DD}(m,r)$ *exists, then*

$$m \leq \frac{\sqrt{\pi}}{2} r + \frac{3\pi^{1/3}}{2^{5/3}} r^{2/3} + O(r^{1/3}) \approx 0.88623r + O(r^{2/3}).$$

- a $\mathrm{DD}(m,r)$ is contained in an anticode $\mathcal{A}$ of diameter at most r and area at most $(\pi/4)r^2$
- cover $\mathcal{A}$ in circles $\mathcal{C}$ of radius ℓ
- count pairs $(\mathcal{C}, d)$ where d is a pair of dots in $\mathcal{C} \cap \mathrm{DD}(m,r)$

Lower Bounds on m

Theorem

There exists a $\mathrm{DD}(m, r)$ *with*

$$m \approx 0.80795r - o(r).$$

Sequences with Distinct Differences

Definition

Let A be an abelian group. A sequence $\{a_1, a_2, \ldots, a_m\} \subseteq A$ is a B_2-sequence if all the sums $a_{i_1} + a_{i_2}$ with $1 \leq i_1 \leq i_2 \leq m$ are distinct.

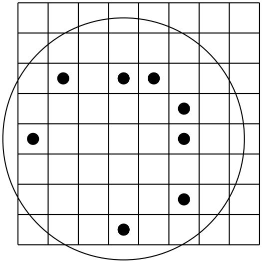
examples:

- Singer difference set
- Golomb ruler
- Bose: B_2-sequence of size q in $\mathbb{Z}_{q^2-1}$

Folding a B_2-Sequence

$\{3, 13, 24, 29, 37, 41, 43, 44\}$
(mod 63)

56	57	58	59	60	61	62	
48	49	50	51	52	53	54	55
40	41	42	43	44	45	46	47
32	33	34	35	36	37	38	39
24	25	26	27	28	29	30	31
16	17	18	19	20	21	22	23
8	9	10	11	12	13	14	15
0	1	2	3	4	5	6	7



Results for the Manhattan Metric

Theorem

- *If a* $\overline{\mathrm{DD}}(m,r)$ *exists then* $m \leq \frac{1}{\sqrt{2}}r + (3/2^{4/3})r^{2/3} + O(r^{1/3})$.
- *There exists a* $\overline{\mathrm{DD}}(m,r)$ *with* $m = \frac{1}{\sqrt{2}}r - o(r)$.

			24			
		17	20	23		
	10	13	16	19	22	
3	6	9	12	15	18	21
	2	5	8	11	14	
		1	4	7		
			0			

- Efficient Key Predistribution for Grid-Based Wireless Sensor Networks, Information Theoretic Security, LNCS 5155, 54 - 69, 2008.
- Distinct Difference Configurations: Multihop Paths and Key Predistribution in Sensor Networks. http://arxiv.org/abs/0811.3896.
- Two-Dimensional Patterns with Distinct Differences – Constructions, Bounds, and Maximal Anticodes. http://arxiv.org/abs/0811.3832.
- Key Predistribution Techniques for Grid-Based Wireless Sensor Networks. http://eprint.iacr.org/2009/014.
- http://www.isg.rhul.ac.uk/~uqah106/

thank you!