Distributed Keys and Agents

Damir Vukičević
Department of Mathematics, University of Split, Croatia

EuroGIGA Final Conference in Berlin, February 17-21, 2014

The first problem

- The system of n keys $K = \{1, \ldots, n\}$
- p persons each possessing some subset $K_i \subseteq K$
- r secure if there is no group of r renegade individuals that can either:
  - read the message (i.e. collect all different keys)
  - disable the rest of persons to read the message

Nuclear suitcase

Example:

- three keys $\{1,2,3\}$
- three persons having key sets $\{1,2\}$, $\{1,3\}$ and $\{2,3\}$
- the system is 1-secure

Torrent

Let us explain this problem in more mathematical way. We are analyzing ordered pairs where the first component is set of $[n]$ the first n positive integers and second component consists of ordered p-tuple $(K_1,...,K_p)$ of the subsets of $[n]$. System is r-secure if it holds that:

A1) $\bigcup_{i\in R} K_i \neq [n]$ for each $R \subseteq [p]$ such that $card(R) \leq r$;

A2) $\bigcup_{i\in [p]\setminus R} K_i = [n]$ for each $R \subseteq [p]$ such that $card(R) \leq r$.

Note that A2) is equivalent to:

A2') each key appears at least $r+1$ times in $K_1,\ldots,K_p$

Let $S \subseteq \mathbb{N}\times\mathbb{N}\times\mathbb{N}$ be the set defined by $(r,p,n)\in S$ if there is at least one r -secure system $([n];K_1,\ldots..,K_p)$. In this case, we say that $([n];K_1,\ldots..,K_p)$ realizes (r,p,n).

Theorem 1. $(r,p,n)\in S \Rightarrow (r,p,n+1)\in S$.

Proof: $\left([n];K_1,\ldots,K_p\right)$ realizes (r,p,n) **implies**

$\left([n+1];K_1\cup\{n+1\},\ldots,K_p\cup\{n+1\}\right)$ realizes $(r,p,n+1)$. ■

S is completely defined by the function $s:\mathbb{N}\times\mathbb{N}\to\mathbb{N}\cup\{+\infty\}$ defined by $s(r,p)=\inf\{(r,p,n)\in S\}$.

Theorem 2. It holds:

1) $s(r,p)=+\infty$ for $p \le 2r$;

2) $s(r,2r+1)=\binom{2r+1}{r}$, for each $r \in \mathbb{N}$;

3) $s(r,p)=r+1$, for $p \ge (r+1)^2$;

4) If $(r,p,n) \in S$, then there is $([n];L_1,\ldots,L_p)$ that realizes (r,p,n) such that each key appears exactly $r+1$ times.

Corollary 3. $s(1,p)=\begin{cases}+\infty, & p\le 2;\\ 3, & p=3;\\ 2, & p\ge 4.\end{cases}$

Theorem 4. $$s(2,p)=\begin{cases}+\infty, & p\le 4;\\ 10, & p=5;\\ 6, & p=6;\\ 5, & p=7;\\ 4, & p=8;\\ 3, & p\ge 9.\end{cases}$$

Theorem 5. It holds:

1) $s(3, p) = +\infty$, for each $p \leq 6$
2) $s(3,7) = 21$;
3) $s(3,8) = 14$;
4) $s(3,9) = 12$;
5) $s(3,10) = 10$;
6) $s(3,11) = 8$;
7) $s(3,12) = 6$;
8) $s(3,13) = 6$;
9) $s(3,14) = 5$;
10) $s(3,15) = 5$;
11) $s(3, p) = 4,\ p \geq 16$.

$s(3,8)=14$

CLAIM: If $(3,p,n)\in\mathbb{N}$, then there are $a_1,a_2,a_3\in\mathbb{N}$ such that $a_1\geq a_2\geq a_3$; $a_1+a_2+a_3\leq n-1$; $p\cdot a_1\geq 4n$; $(p-1)\cdot a_2\geq 4(n-a_1)$; $(p-2)\cdot a_3\geq 4\cdot(n-a_1-a_2)$.

$p \cdot a_1 \geq 4n$

Proof: It is sufficient to take a_1 as the largest cardinality of K_i (let us denote that set with K_{b_1}),

P_{b_1}	*	*	*				
P_{b_2}							
P_{b_3}							
...							

$(p-1)\cdot a_2 \geq 4(n-a_1)$, $a_1 \geq a_2$

a_2 as the largest cardinality of $K_i \setminus K_{b_i}$ (let us denote such set of keys with K_{b_2})

P_{b_1}	*	*	*				
P_{b_2}			.	*	*		
P_{b_3}					.		
...							

$$(p-2)\cdot a_3 \geq 4\cdot(n-a_1-a_2);\ a_2 \geq a_3;\ a_1+a_2+a_3 \leq n-1$$

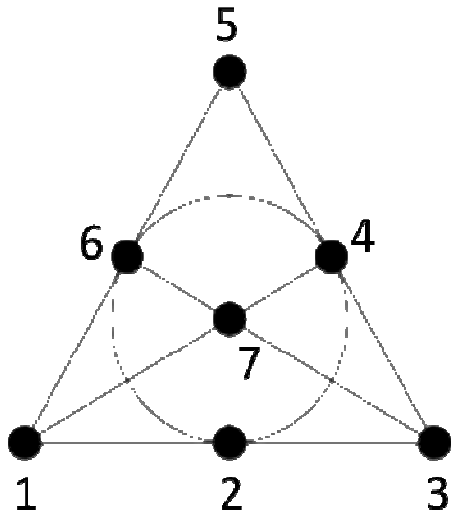
and a_3 as the largest cardinality of $K_i \setminus \left(K_{b_1} \cup K_{b_2}\right)$. ■

P_{b_1}	*	*	*				
P_{b_2}			.	*	*		
P_{b_3}					.	*	
...							

From this claim it directly follows that $(3,8,n) \notin S$ for $3 \leq n \leq 13$.

Direct computer check using three for-loops respectively for a_1, a_2 and a_3 .

It remains to show that $(3,8,14)$ can be realized. We construct $\{[14]; K_1, \ldots K_8\}$ that realizes $(3,8,14)$.



These plane consists of 7 lines (circle is counted as a line) and has the following properties:

F1) each line has exactly three points;

F2) each point lies on the exactly three lines;

F3) each two lines intersect at exactly one point;

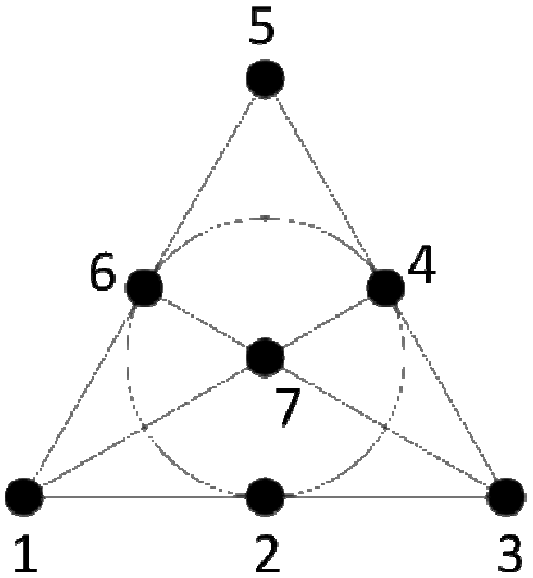
F4) If three lines cover all the points, then they intersect at one point.

Lines $K_1,\ldots,K_8$ are given in the following way:

1) each K_i, $i=1,\ldots,7$ corresponds to one line l_i in the following way.

$$K_i=\{x: x\in l_i\}\cup\{x+7: x\notin l_i\};$$

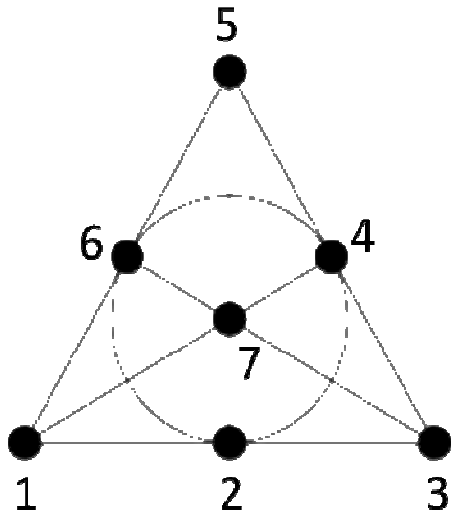
2) $K_8=\{1,2,3,4,5,6,7\}$.



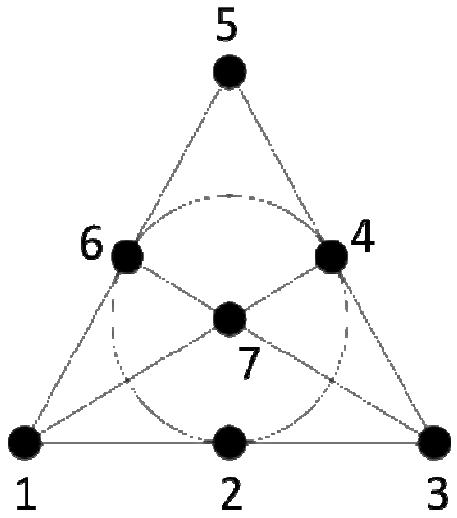
e.g.

1,2,3-> 1,2,3,11,12,13,14

2,5,7->2,5,7,8,10,11,13

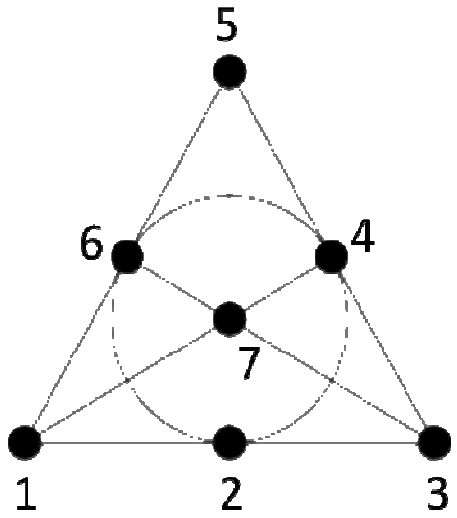


Note that there are four copies of each key, hence A2') holds. Let us show that A1) holds. Suppose to the contrary that there are three renegades that can read the whole message.



CASE 1: Person 8 is in the group. (he has keys $\{1,2,3,4,5,6,7\}$)

The remaining two persons correspond to two lines that intersect in one point, say q. Then, this group does not have key $q+7$.



CASE 2: Person 8 is not in the group

Lines corresponding to the persons in this group intersect at one point (say q) because they must have all the keys in $[7]$ and again this group does not have key $q+7$.

This proves that $s(3,8)=14$.

Additional results

Parliament application – 303 representatives, 152 votes required

$$\log_{10}\binom{303}{151} \approx 91.2$$

Theorem 6. Let $x \geq 10$ and let $(x, 3x, n) \in S$, then

$$n \geq \frac{(x^2 - x - 2) \cdot \left(\frac{25}{9}\right)^{\left\lfloor \frac{x-1}{2} \right\rfloor}}{4x^2 - 2x} + 1 .$$

Hence: There should be more than $3.8 \cdot 10^{21}$ keys for the parliament of 303 representatives

The second problem

- Organization wants to plant group of “sleepers”
- Sleeper = spy that lives normal life until they are called to perform some mission
- After they get a message they have to go to certain location and do their mission that is revealed to them

- Location and mission is protected by a secret code that can be unlocked by a series of keys
- Each sleeper can have some (or none) of the keys
- Each of sleepers knows only some of his colleagues

- These sleepers can be represented as a graph in which edges connect pairs of sleepers that know each other.
- The mission can obviously be implemented if there is a connected component of this graph that has all the keys

- The aim is to make a network that is resilient to adversary's agents planted in the sleepers group.
- It is assumed that if there is the adversary agent, he will betray all the sleepers that he knows and give his keys to the adversary

- Network is r resilient if no r persons acting as adversary agents can either collect all the keys or break the graph in such a components that no component has all the keys.
- Our aim is to determine for the given triplet of numbers (a, p, k) whether there is a network with p persons and distribution of k keys in that network such that it is resilient to the attack of any a agents.

Mathematical reformulation:

We are searching for the set $S \subseteq \mathbb{N}^3$ such that $(a, p, k) \in S$ if and only if there is a graph $G = (V, E)$ with p vertices and function $\kappa : V \to P(\{1, \ldots, k\})$ such that for each set $A \subseteq V$ with a vertices it holds:

A1) $\bigcup_{v \in A} \kappa(v) \neq \{1, \ldots, k\}$;

A2) there is a component C of the graph $G \setminus M_G(A)$ such that $\bigcup_{v \in C} \kappa(v) = \{1, \ldots, n\}$.

Theorem 7. It holds:

1) $(a,p,k)\in S \Rightarrow (a,p+1,k)\in S$;

2) $(a,p,k)\in S \Rightarrow (a,p,k+1)\in S$.

Theorem 8. It holds: $K(1,p)=\begin{cases}+\infty, & p\le 3;\\ 2, & p\ge 4.\end{cases}$

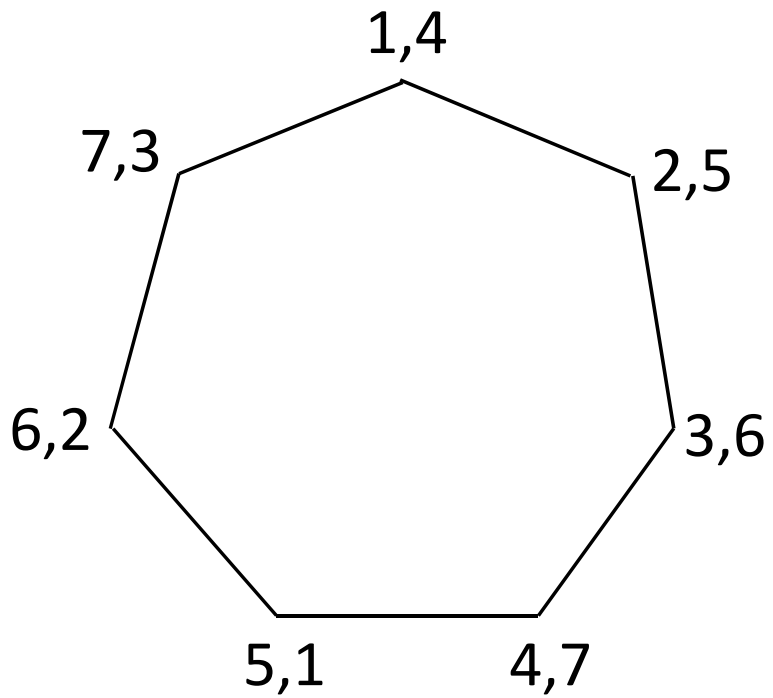
Theorem 9. It holds: $K(2,p)=\begin{cases}+\infty, & p\le 8;\\ 3, & p\ge 9.\end{cases}$

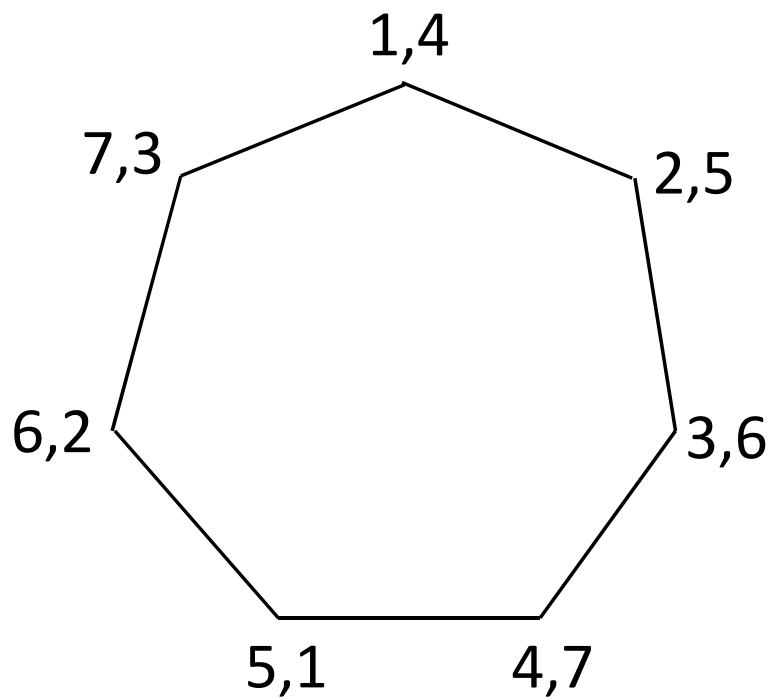
Theorem 10. It holds $K(3,p)=\begin{cases}+\infty, & p\le 13;\\ 7, & p=14,15;\\ 4, & p\ge 16.\end{cases}$

$K(3,p)=7,\ \ p=14,15$

- $(3,14,7)$ can be realized
- $(3,15,6)$ can not be realized

Realization (G, κ) of $(3,14,7)$





$(3,15,6)$ can not be realized

CASE 1: There are three components with at least 4 vertices.

CASE 2: There are two components with at least 4 vertices.

CASE 3: There is exactly one component C_1 with at least 4 vertices.

Claim A. Let G be a graph with at most 7 vertices different from cycle $C(7)$, $k \in \mathbb{N}$, and $\kappa : V(G) \to \{1,\ldots,n\}$ function. Then either, there are three vertices $v_1, v_2, v_3 \in V(C(7))$ such that $\kappa(v_1) \cup \kappa(v_2) \cup \kappa(v_3) = \{1,\ldots,k\}$ or there is a vertex v_0 such that for every connected component C of $G \setminus M(v_0)$, it holds that $\bigcup_{v \in C} \kappa(v) \neq \{1,\ldots,n\}$.

Claim B. Let $\kappa: V\left(C(7)\right) \to \{1,\ldots,6\}$ be the function. Then either, there are three vertices $v_1, v_2, v_3 \in V(G)$ such that $\kappa(v_1) \cup \kappa(v_2) \cup \kappa(v_3) = \{1,\ldots,6\}$ or there is a vertex v_0 such that for every connected component C of $G \setminus N(v_0)$, it holds that $\bigcup_{v \in C} \kappa(v) \neq \{1,\ldots,6\}$.

If this component is either a cycle or a path, there is a set of three vertices $A=\{w_1,w_2,w_3\}$ such that no component of $C_1 \setminus M(A)$ has more than 2 vertices, but then A1) implies that no component has all the keys contradicting A2).

Therefore, we may assume that there is a vertex in C_1 of cardinality at least 3. Hence, $C_1 \setminus M(w_1)$ has at most 11 vertices. If $C_1 \setminus M(w_1)$ is either a cycle or a path, then there are vertices w_2 and w_3 such that $(C_1 \setminus M(w_1)) \setminus M(\{w_2, w_3\})$ has no component of cardinality larger than 3. Fruther, A1) implies that no such component has all the keys, but then no component of $G \setminus M(\{w_1, w_2, w_3\})$ has all the keys which contradicts A2).

Hence, we may conclude that $C_1 \setminus N(w_1)$ has a vertex w_2 of degree at least 3, but then graph $(C_1 \setminus M(w_1)) \setminus M(w_2) = C_1 \setminus M(\{w_1, w_2\})$ has at most 7 vertices.

From A1) and Claims A and B, it follows that there is a vertex w_3 such that no component of $C_1 \setminus N(\{w_1, w_2\}) \setminus N(w_3)$ has all the keys, but then no component of $G \setminus N(\{w_1, w_2, w_3\})$ has all the keys which contradicts A2).

Theorem 11. $K(4, p) = +\infty$ for $p \leq 20$.

Theorem 12. $K(4,21)=10$.

$$K(4,25)=5$$

$$K(4,22), K(4,23), K(4,24) = ??$$

Thank you for your attention