Identification Systems
Lecture 6

Piotr Syga

2021-04-20

Wireless sensor networks – basic idea

- severely constrained devices that collect and transmit environmental data
- small size and cost of a single device – frequent device malfunctions may appear
- active transmission, broadcast communication
- limited energy
- limited memory with severely constrained writable section
- limited computation power – no PKI
- stationary vs mobile/ad hoc networks

Important components

Microcontroller – typically field programmable gate arrays,application-specific integrated circuits or digital signal processors

Transceiver – transmitter–receiver that works on ISM bands (UHF: 902–928 MHz, S-band: 2.4–2.5 GHz, C-band: 5.725–5.875 GHz) – data rate in modern sensors varies from 250Kbps to 1Mbps

Memory – typically a flash drive for storing the data, the codes and temporary data of the protocols, identification data is usually stored in the microcontroller

Battery – often divided into primary (not rechargeable) and rechargeable secondary power sources, most of the energy is spent on the transmission

Examples



Figure: MICAz ZigBee sensor

Examples



Figure: ATsensor based on COTS

Examples

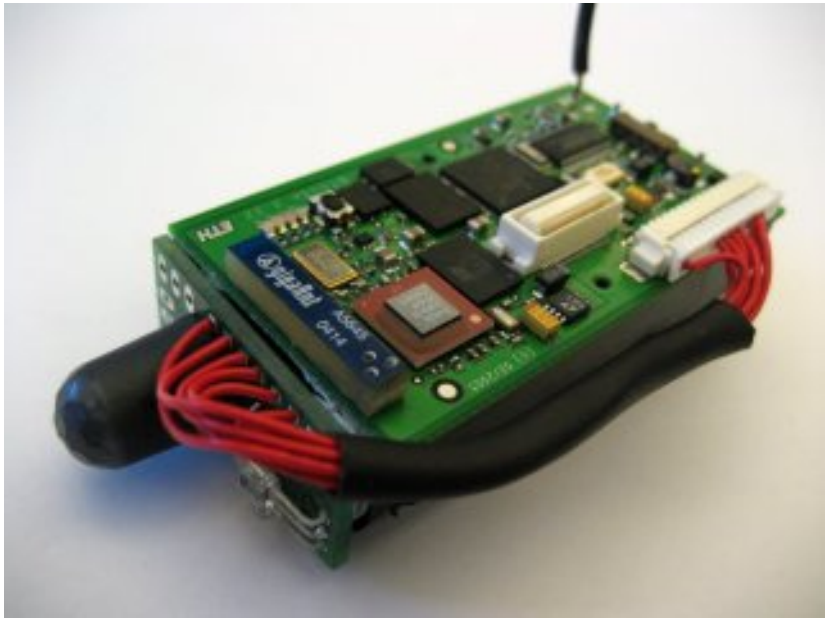


Figure: BTnode Sensor

Classification

Sensor capability – memory size, authorization method, data verification, tamper-resistance, power sources etc.

Setup and Mobility – random distribution vs predeployment, grid vs scatter, stationary vs mobile

Routing destination – a single sink, multiple sink, active aggregator, spreading the information across the network

Data source – environmental monitoring vs event-driven

Connectivity – singlehop vs multihop, landbridges vs redundancy

Special cases of networks of usually stronger devices: Vehicular ad hoc networks, self-stabilizing mobile ad hoc network

Parameters

- Spatial resolution
- Temporal resolution
- Latency
- Coverage
- Bandwidth
- Control-Supervision
- Uniformity of the nodes
- Cooperation type of the nodes
- Lifetime
- Sense of occurrence

Communication models

- Multiple Access Channel
- Carrier Sensing
- Signal-to-noise ratio, signal-to-interference-plus-noise ratio
- LoRa models

An example of translation between MAC and SINR models may be found in Jurdzinski, Kowalski: *Distributed Backbone Structure for Algorithms in the SINR Model of Wireless Networks*

Limitations

- constrained computational power – no PKI
- constrained battery capacity – limited number of messages
- limited memory – cannot store a dedicated key for each pair
- eavesdropping and node-capturing adversary – requirement for encryption and prevents 'universal key'
- network may be singlehop – the goal is to create a secure connection between each two nodes
- ad hoc environment – new nodes may join with limited or no possibility to new keys to previous nodes

Key Predistribution

Idea by Eschenauer and Gligor (*A key-management scheme for distributed sensor networks*)

- We generate a large keypool P of size N.
- Every node stores a random subset of P of size n
- Due to Birthday Paradox, if $n = O(\sqrt{N})$ every two nodes share a common key whp.
- To establish the connection, nodes exchange (openly) the IDs of their keys

The idea was extended over the years including q-composite keys (Chan et al.), key evolution, eg., using Merkle trees (Su et al.) or key levels (Cichoń et al.) and many more.

Combinatorial Design

Camtepe, Yener: *Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks*

- Using a symmetric Balanced Incomplete Block Design in order to predistribute keys to each node.
- General construction for combinatorial design focusing on Finite Projective Planes.
- Ensuring that each pair of the nodes have exactly one shared key.
- Reducing the size of the subset of P stored in each node.
- Limited number of unique keypools for nodes.

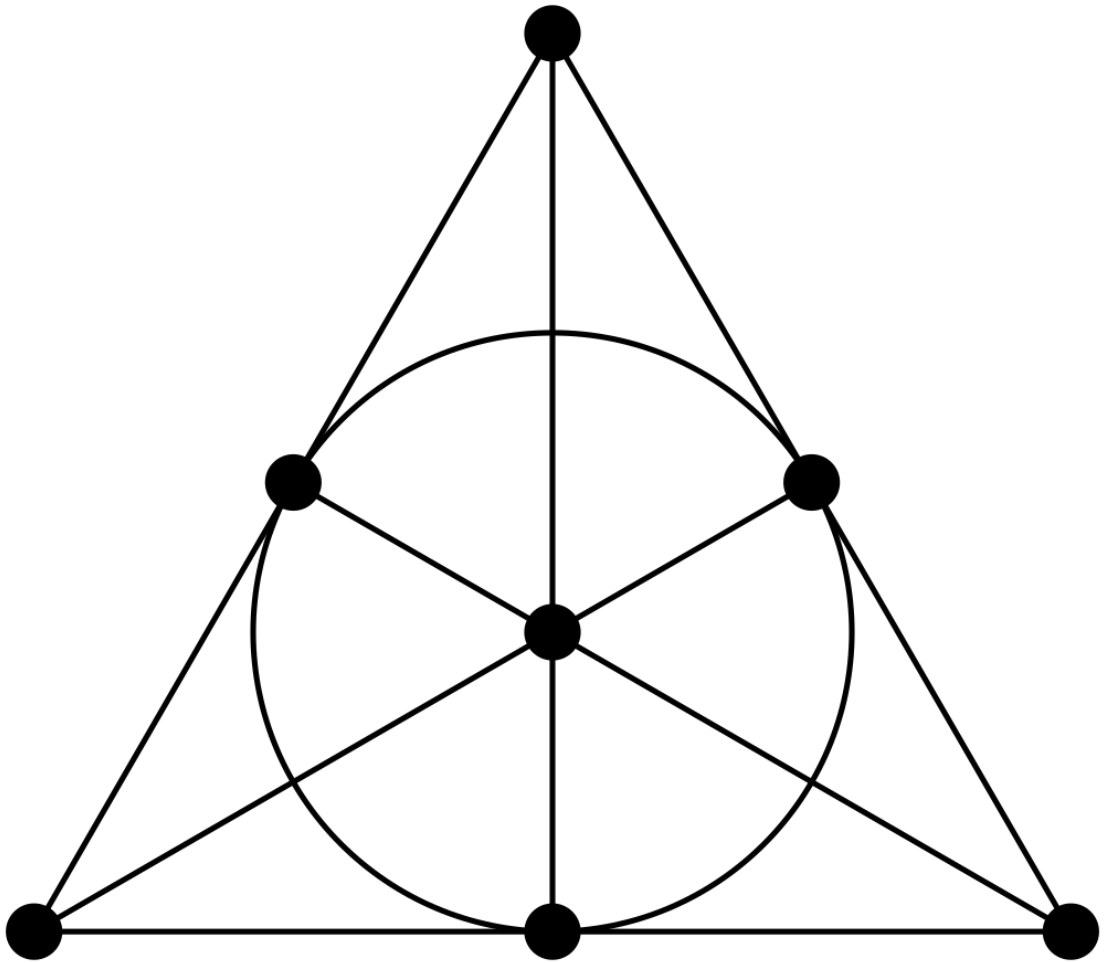
Combinatorial Design

Projective Planes

- Two dimensional space consisting of two disjoint sets – points, and lines.
- Projective plane of order q has exactly $q^2 + q + 1$ points and $q^2 + q + 1$ lines.
- There are exactly $q + 1$ points on each line, each point belongs to $q + 1$ lines.
- Each two lines intersect (share a point) and each two points have a line that includes them.
- One can easily derive a dual plane.

Combinatorial Design

Fano Plane ($PG(2,2)$)



Combinatorial Design

Mapping

Symmetric, GQ and Hybrid Designs		Key Distribution
Object (Point) Set	$\rightarrow$	Key-Pool (P)
Object (Point) Set Size v	$\rightarrow$	Key-Pool Size ($\|P\|$)
A Block (Line)	$\rightarrow$	A Key-Chain
# Blocks (Lines) b (+ # random blocks of Hybrid Design)	$\rightarrow$	# Key-Chains and # Sensor Nodes (N)
# Objects (Points) in a Block (Line)	$\rightarrow$	# Keys in a Key-Chain (K)
# Blocks (Lines) that an Object (Point) is in	$\rightarrow$	# Key-Chains that a Key is in
Two Blocks (Lines) share λ Object (Points)	$\rightarrow$	Two Key-Chains share (χ) Keys

Combinatorial Design

BIBD

- a generalization of PG – a tuple (v, b, r, k, λ)
- arranges v different objects into b blocks
- each block contains exactly k distinct objects, each object occurs in exactly r different blocks
- each pair of distinct objects occurs together in exactly λ blocks
- symmetric BIBD assumes $v = b$ and $k = r$

Combinatorial Design

Finite Generalized Quadrangle

$GQ(s, t)$ is a structure describing incidence between set of points P and blocks B that are disjoint and non-empty, and a (symmetric) point to block relation, such that:

- Each point is incident with $t + 1$ blocks and 2 distinct points are incident with at most one block.
- Each block is incident with $s + 1$ points and 2 distinct blocks are incident with at most one point.
- If p is a point and L a block that is not incident with p, then there is a unique pair (y, M) such that M is incident with both x and y and y is incident with L

Combinatorial Design

Security

- One can observe that if the Adversary compromises x nodes, the probability that a link between two honest nodes is compromised is equal to $\sum_{i=1}^{k} (1 - (1 - \frac{k}{|P|})^x)^i \frac{p(i)}{p}$, where $|P|$ is the size of the keypool, k is the size of keychain, $p(i)$ is the probability of establishing connection with i keys and $p = p(1) + \cdots + p(k)$.
- Note that for projective planes, the probability of establishing connection is always 1.
- Moreover, the probability that a connection secured with key i if it is secure $\Pr(I_i|I) = \frac{\binom{q+1}{2}}{\binom{q^2+q+1}{2}} = \frac{1}{q^2+q+1}$
- Probability that at least one of compromised blocks contains the key i is $1 - \frac{\binom{q^2}{x}}{\binom{q^2+q+1}{x}}$.
- Hence the probability of compromising the connection is equal to $\sum_{j=1}^{q^2+q+1} (1 - \frac{\binom{q^2}{x}}{\binom{q^2+q+1}{x}}) \Pr(I_i|I) = 1 - \frac{\binom{q^2}{x}}{\binom{q^2+q+1}{x}}$

Combinatorial Design

Results

Design	Pool Size	Key Chain Size	Number of Sensors	Random Prob.	Symmetric/GQ/ Hybrid Prob.	Random Avg. Key-Path	Symmetric/GQ/Hybrid Avg. Key-Path	Avg. Node Degree
Symmetric	100807	318	100807	0.634	1.0	–[a]	1.0	–
	10303	102	10303	0.639	1.0	1.35	1.0	56
	5113	72	5113	0.642	1.0	1.35	1.0	51
	2863	54	2863	0.645	1.0	1.35	1.0	47
	1407	38	1407	0.651	1.0	1.34	1.0	42
	553	24	553	0.663	1.0	1.33	1.0	35
$GQ(q,q)$	7240	20	7240	0.053	0.052	2.68	2.69	205
	5220	18	5220	0.060	0.058	2.89	2.88	148
	2380	14	2380	0.079	0.076	3.17	3.18	88
	1464	12	1464	0.094	0.090	2.73	2.71	81
	400	8	400	0.150	0.140	3.61	3.49	32
	156	6	156	0.212	0.192	2.82	2.53	25
$GQ(q,q^2)$	15984	12	162504	0.009	0.009	–	–	–
	2753	8	17200	0.023	0.022	2.96	2.96	631
	756	6	3276	0.046	0.045	3.12	3.22	179
	112	4	280	0.137	0.128	5.63	5.49	29
	27	3	45	0.308	0.266	2.23	2.14	15
$GQ(q^2,q^3)$	81276	26	393876	0.0083	0.0083	-	-	-
	2440	10	6832	0.0403	0.0395	2.68	2.68	366
	165	5	297	0.1443	0.1347	2.75	2.69	43
Hybrid	10303	102	10500	0.639	0.99	1.36	1.01	56
	5113	72	5250	0.642	0.99	1.35	1.01	51
	2863	54	3000	0.645	0.98	1.35	1.03	47
	1407	38	1500	0.651	0.97	1.34	1.04	42
Symmetric	553	24	750	0.663	0.89	1.33	1.15	37
	183	14	250	0.685	0.89	1.31	1.14	29

[a] We only provide analytical solution for probability of key share for the networks larger than 10000 nodes due to memory limitations.

Privacy during key establishment

- Key predistribution allows us to ensure (or increase the probability) that every nodes share a common key, yet it is not enough to establish secure and private communication.
- One may note that in the KDS, each keychain is either unique or the probability of the collision is negligible.
- If each node transmits the IDs of its keys, they become de facto node ID, hence the adversary may track mobile sensor.
- We want to establish a connection between two nodes, and provide some tracking prevention.

Privacy during key establishment

The problem of uniqueness

Let us assume that we have a network utilizing the protocol Eschenauer and Gligor, with keypool of size N and $c\sqrt{N}$ keys assigned randomly to each of m nodes in the system. Then the probability that there are two nodes with the same subset of keys i.e., $\mathcal{K}^{(A)} = \mathcal{K}^{(B)}$ for some two nodes $A \neq B$, does not exceed $m^2 \cdot (c/\sqrt{N})^{c(\sqrt{N})}$.

Privacy during key establishment

M. Klonowski, PS: *Enhancing Privacy for Ad Hoc Systems with Predeployment Key Distribution*

Model

- the sensors are mobile
- communication is bilateral (via unicast)
- each sensor A has its keypool $\mathcal{K}^{(A)}$ of size n
- no specific KDS is assumed
- nodes can use PRNG and compute some standard symmetric encryption and decryption
- nodes do not know their position nor the identifiers of any (including themselves) node

Privacy during key establishment

Adversary

Weak Passive Adversary (WPA) - its acting is limited to intercepting all the messages exchanged between communicating nodes. Initially it has no knowledge about keys from the keypool. However it can use observations of previous communications for establishing identities of communicating parties.

Strong Passive Adversary (SPA) - additionally to the capabilities of WPA, the adversary posses some keys from the key pool $\mathcal{K}^{(Adv)} \subset \mathcal{K}$, however they cannot predict random choices of any communicating parties. Moreover it does not interrupt or initiate communication between parties.

Active Adversary (AA) - controls some of communicating devices (as well as keys they possess) and can initiate and conduct communication with random subset of nodes in order to establish information about other devices.

Privacy during key establishment

Table: The summary of the notation

Symbol used	Meaning
m	number of nodes in the network
$\mathcal{K}$	set of all possible keys
N	size of $\mathcal{K}$
$\mathcal{K}^{(A)}$	individual keypool of node A
$\mathcal{K}_t^{(A)}$	individual keypool of node A in epoch t
n	size of each individual keypool
k_j	j^{th} key of global keypool
$k_j^{(A)}$	j^{th} key in the keypool of node A
$x \in_R L$	x is chosen at random from the set L
$a\|\|b$	concatenation of strings a and b
$\|a\|$	number of bits in a
$\mathrm{Enc_k}(\mathrm{msg})$	encryption of message *msg* using key k
$\mathrm{Dec_k}(\mathrm{msg})$	decryption of message *msg* using key k
$H(x)$	invoking one way hash function on input x
$\mathrm{BF}_{(h_1,\ldots,h_K)}(e_1,\ldots,e_n)$	Bloom Filter using hash functions $h_1, \ldots, h_K$ representing the set $\{e_1,\ldots,e_n\}$
$\mathrm{BF}[x]$	x-th bit of the Bloom Filter

Privacy during key establishment

Unlinkability game

- Let us assume nodes from the set $\{1, \ldots, m\}$.
- The adversary observes T consecutive key establishment sessions and i_t^1, i_t^2 denote nodes participating in the t-th session.
- Let $O(i_1^1, i_1^2, \ldots, i_T^1, i_T^2)$ denote the sequence of observations generated by $\{i_t^1, i_t^2\}, \ldots, \{i_T^1, i_T^2\}$.
- Let us consider following game with respect to observations t_1, t_2
  - The adversary chooses any $I = (i_1^1, i_1^2, \ldots, i_{t_1}^1, i_{t_1}^2, \ldots, i_{t_2}^1, i_{t_2}^2 \ldots, i_T^1, i_T^2)$ and a pair $\{i_{t_2}'^1, i_{t_2}'^2\}$ such that $\{i_{t_1}^1, i_{t_1}^2\} \cap \{i_{t_2}^1, i_{t_2}^2\} = \emptyset$ and $\{i_{t_1}^1, i_{t_1}^2\} \cap \{i_{t_2}'^1, i_{t_2}'^2\} \neq \emptyset$.
  - Let

$$\begin{aligned} O_0 &:= O(i_1^1, i_1^2, \ldots, i_{t_1}^1, i_{t_1}^2, \ldots, i_{t_2}^1, i_{t_2}^2 \ldots, i_T^1, i_T^2), \\ O_1 &:= O(i_1^1, i_1^2, \ldots, i_{t_1}^1, i_{t_1}^2, \ldots, i_{t_2}'^1, i_{t_2}'^2, \ldots, i_T^1, i_T^2). \end{aligned}$$

  - A random bit b is chosen and the adversary is given O_b. The aim of the adversary is to guess b.
- Note that O_0 and O_1 differ only on the IDs of nodes communicating in observation t_2.

Privacy during key establishment

Strong Unlinkability

We say that observation t_1 is **strongly unlinkable** to observation t_2 if for any PPT algorithm $\mathcal{A}$, any set I and any pair $\{i'^1_{t_2}, i'^2_{t_2}\}$

$$\Pr[\mathcal{A}(O_b, I, \{i'^1_{t_2}, i'^2_{t_2}\}) = b] < 1/2 + \varepsilon(I),$$

where the adversary's advantage - $\varepsilon(I)$ is a negligible function of the security parameter I.

Privacy during key establishment

Protocol for WPA

The protocol of finding the common key between the nodes A and B proceeds as follows:

1. A chooses random nonce $\eta \in \{0,1\}^l$,
2. A computes $\mathrm{BF} := \mathrm{BF}_{h_1,\ldots,h_K}(\eta||k_1^{(A)}, \ldots, \eta||k_n^{(A)})$,
3. A sends the pair (BF, η) to B,
4. for each $k_i^{(B)} \in \mathcal{K}^{(B)}$, B calculates

$$x_{1,i} = h_1(\eta||k_i^{(B)}), \ldots, x_{k,i} = h_K(\eta||k_i^{(B)}) \ .$$

5. If there is exactly one key $k_i^{(B)}$, for which all $\mathrm{BF}^{(t)}[x_{j,i}] = 1$ for each j, the $k_i^{(B)}$ is the common key and is used for communication. Otherwise "error message" $\perp$ is returned to B and the procedure is restarted with new t.
6. When A receives the message,
   - new random value η is selected if it was an "error message" $\perp$;
   - A tries to decrypt the received message with all $k_i^{(A)}$ proceeds with encrypted communication.

Privacy during key establishment

Communication Complexity

For the number of keys greater than $n > 70$ the expected number of bits exchanged, necessary to find the common key is smaller than $1.5(n \log n + l)$.

Privacy during key establishment

Unlinkability

Let us assume $T = O(\text{poly}(l))$ the protocol has been observed by the adversary. Then **all** observations are strongly unlinkable to all other observations.

Proof

Let us note that sent messages are result of independent hash functions invoked for nonces concatenated with keys unknown to the adversary and that for any $i \neq j$ we have keychains of equal sizes s.t. $\mathcal{K}^{(i)} \cap \mathcal{K}^{(j)} = 1$. Thus, even if the adversary could observe all the results, they are values of hash functions of unknown arguments used only once, thus they can be treated as random values independent of any previous and future communication. The only problem that may appear when the same nonce η is used twice. Note however that there is at most polynomially many number of observations. Using union-bound argument the probability of the event is at most $\varepsilon(l) = O((1.9)^{-l})$, thus is negligible.

Privacy during key establishment

Protocol for SPA

- assumes the occurrences of safe rounds
- during the safe rounds, nodes select a subset of keys and exchange each with probability $\frac{1}{2}$
- if KDS assures that each keychain shares at least one key with any other (e.g. $PG(2, q)$, $GQ(q, q)$), we preserve the property whp
- coupling based proofs on the bound of safe rounds

Privacy during key establishment

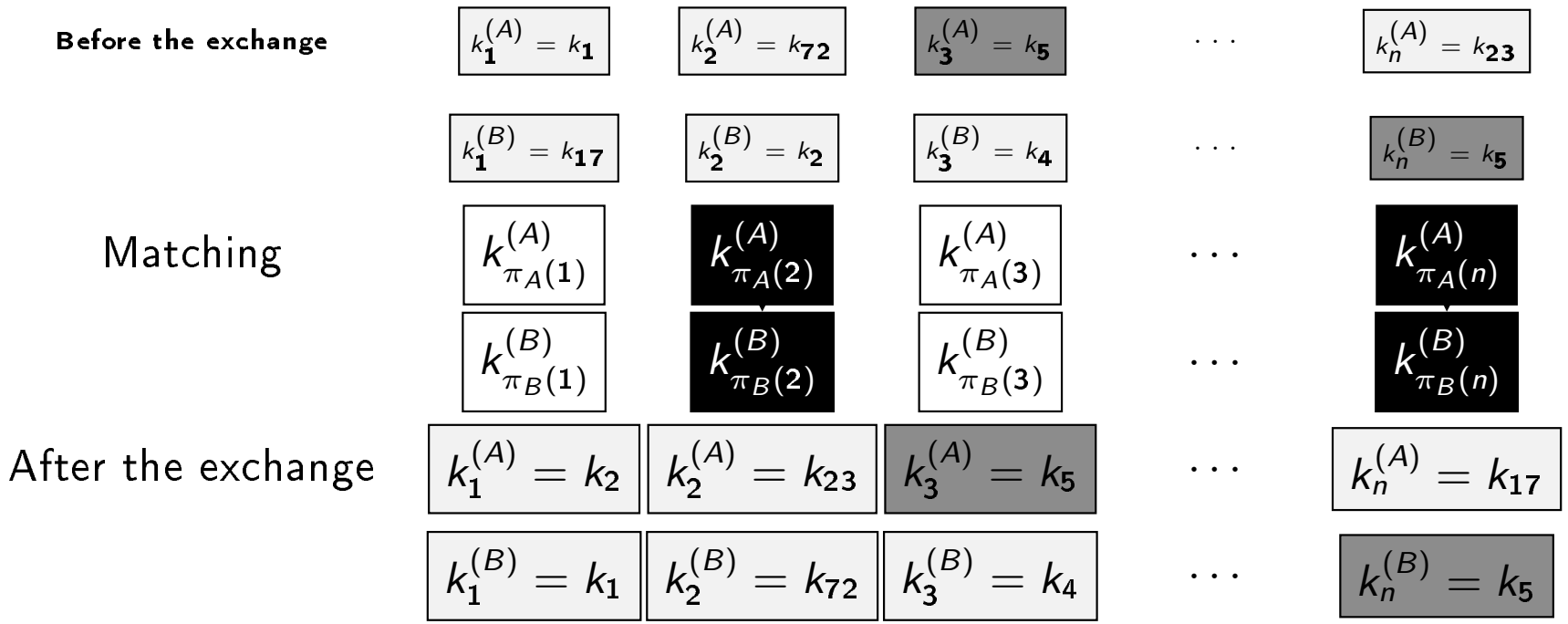


Figure: Dark gray rectangle denotes the common key that may not be exchanged. Black rectangles depict the keys to be exchanged, white depict those keys that were paired together but will not be exchanged.