Forward-secure Key Evolution in Wireless Sensor Networks

Marek Klonowski[1], Mirosław Kutyłowski[1], Michał Ren[2], and Katarzyna Rybarczyk[2]

[1] Wrocław University of Technology
[2] Adam Mickiewicz University, Poznań, Poland

Abstract. We consider a key distribution scheme for securing node-to-node communication in sensor networks. While most schemes in use are based on random predistribution, we consider a system of dynamic pairwise keys based on design due to Ren, Tanmoy and Zhou. We design and analyze a variation of this scheme, in which capturing a node does not lead to security threats for the past communication. Instead of bit-flipping, we use a cryptographic one-way function. While this immediately guarantees forward-security, it is not clear whether the pseudorandom transformation of the keys does not lead to subtle security risks due to a specific distribution of reachable keys, such as existence of small attractor subspaces. (This problem does not occur for the design of Ren, Tanmoy and Zhou.) We show, in a rigid mathematical way, that this is not the case: after a small number of steps probability distribution of keys leaves no room for potential attacks.

keywords: communication in sensor networks, key management, key distribution, forward security, directed random graphs

1 Introduction

Applications of sensor networks are sometimes constrained by security requirements. In order to be attractive from economic point of view, nodes of a sensor network need to be very cheap. This results in lack of tamperproofness (and tamper-resistance), limited computing power and memory space, inability to perform public-key cryptography efficiently, and limited communication bandwidth (due to battery capacity). This creates challenges for communication security: no public-key cryptography can be used, only symmetric algorithms are admissible, communication volume of the security protocols should be kept as small as possible. However, one of the crucial security threats in sensor networks is that communication can be recorded and the secret keys can be retrieved from a captured device. This may lead to disclosure of all data sent so far with the keys contained in this device. On the other hand, lack of connection to the device captured is nothing uncommon – it can be due to battery exhaustion or any physical failure. Also, it might be hard to find a device that is not responding to radio signals, so it is difficult to check if a device has been captured.

Recently, a simple scheme of dynamically evolving keys [1] has been proposed. It supports pairwise symmetric keys for each pair of communicating nodes, which change the key at every transmission. Namely, the sender chooses a key bit at random, flips it, and encodes current data transmission with the obtained key. The receiver makes trial decryptions and, based on the results, recovers which bit has been changed.

The idea of this solution is remarkably simple; it is both efficient and easy to implement. Obviously, in this way it only takes a small number of steps to change a key into any other key. This solves a lot of problems – for instance if some encrypted transmission has been recorded and cryptanalysis reveals the key used for encryption, it cannot be used to eavesdrop later transmissions. Simply, in the meantime the sensors transformed their keys completely. An attack in this case requires uninterrupted monitoring communication activities of a sensor. Replay and replication attacks become very limited. A nice feature especially for the sensor networks is that there is no communication overhead due to evolution of keys – this is important, since energy consumption for communication is of order of magnitudes higher than for any internal computations by the processor. For further discussion see the original proposal [1].

Problem Description The major weakness of the scheme [1] is that if the current key is compromised, and the adversary has recorded the traffic beforehand, it is possible to reverse key transitions step by step. Our goal is to design an efficient framework that shares all advantages of the scheme from [1], but is resistant to the mentioned security threat.

Previous work Since the most energy-intensive operation for a sensor node is wireless communication, protocols dedicated to the sensor networks should be optimized with respect to communication volume. Sending a bit is a typically orders of magnitude more expensive than encryption or decryption. On a specialized hardware, energy cost of $9nJ$ per bit is achievable for AES encryption [2], but sending a bit requires around 21 μJ, which is a difference of three orders of magnitude. It is to be expected that the relative difference will increase as processor technology matures; in fact, modern optimized hardware achieves energy costs of AES encryption on order of $60pJ$ per bit [3]. For these reasons any key management protocol should avoid large communication overhead, and most solutions designed for wired networks (such as the SSL protocol) are useless in the context of sensor networks. The second limitation of this type is memory size and communication speed. A typical sensor network node has no more than 4KB of memory, and is capable of communicating at speeds of about 38.4 Kbps to a distance of around 30m. The nodes are also usually equipped with coprocessors to handle AES encryption and decryption efficiently. Asymmetric methods, on the other hand, require millions of multiplications per asymmetric operation, as well as large amounts of memory and currently are not considered suitable for sensor networks.

Most of the recent work on the problem of key distribution and management in sensor networks has been focused on random predistribution schemes (see e.g. [4–6]). Let us recall their general framework:

1. *Key predistribution phase* is conducted offline. It consists of generating a large pool of keys and loading a small number of different randomly-drawn keys into each sensor device. An identifier should be assigned to each key.
2. *Shared key discovery phase* takes place in the target environment, after the sensor nodes are deployed. Every node discovers its neighbors, and tries to establish a common key with each neighbor. The simplest method of achieving this goal is that each node broadcasts in plaintext the list of identifiers of all keys it possesses. This phase establishes network topology, as two nodes are "linked" only if they share at least one pre-installed key.
3. *Path-key establishment phase* allows pairs of nodes that are in communication range to establish a common key, even if they did not share any after the previous phase.

Adversary model for sensor networks has some peculiarities. Due to reliance on radio communication it is quite easy to record the traffic, or at least a part of it. The second point is that it is hardly possible to prevent an adversary from compromising some of the sensor nodes and extracting their keys. Moreover, due to failures occurring in usual field conditions, lack of response from a node might be regarded as a normal failure. Checking a node on-site is seldom possible. This is a serious problem for predistribution schemes. In case of compromising a node all its keys should not be used anymore. However, in practice, is it hard to distinguish between node compromise and battery exhaustion or any other failure. Large pools of keys help a little: only a fraction of traffic becomes insecure in this way.

On the other hand, some assumptions about the capabilities of the adversary can be relaxed in the context of sensor nodes. For example, it can be assumed that an adversary is not omnipresent and can not eavesdrop on all communication links all the time. This allows for construction of counterintuitively secure protocols, such as the key infection protocol, which is based on broadcasting the keys in the clear [7]. We can assume that in real-world scenarios within a few seconds immediately after deployment of the network, the adversary is unable to eavesdrop on all communications, but only a certain fraction of them.

The solution presented in [1] works with keys that are derived dynamically from the initial pairwise keys (which might be established in the clear or be derived from predistributed keys). The principal advantage is that evolution of the pairwise keys does not require any communication overhead. It is performed at a very modest energy cost, provided that encryption and decryption could be done efficiently. It also forces the adversary to keep monitoring communication all the time after compromising a key; otherwise the adversary loses control of the key as it diverges.

2 KEP – Key Evolution Protocol

Initialization As in [1], the system initializes the nodes so that each pair of neighbor nodes establishes a key for this pair. Any method can be used: preloading with a common key, key infection, or a random predistribution scheme. At the end of this phase, every node knows its neighbors and shares a separate pairwise key with each neighbor.

Communication with Key Divergence Consider nodes A and B sharing a pairwise key, say k_{AB}. We describe the steps executed by A. It waits until either it sends a message to B, or it receives one addressed to itself from B.
Case 1: A initializes key transition while sending a message to B
The following steps are executed:

1. A encrypts the message to be sent with a key k', called *proposed key*, that is derived from k_{AB} as follows:
$$k' := F(k_{AB}, i) \tag{1}$$
where F is a cryptographic one-way function and $i \leq l$ is chosen uniformly at random. The parameter l is a small constant, $l \geq 2$, controlling convergence rate. In the second version of the protocol
$$k' := F(k_{AB}, i, t) \tag{2}$$
for t denoting the so called *current index of* k_{AB}. Initially, this index is set to 1, and then increased after each transformation of k_{AB}.
2. If A has to send more messages, but has not yet received a message from B (neither valid nor invalid), it sends every next message encrypted to proposed key k'.
3. Finally, A receives a message from B. If it is encrypted to proposed key k' and the message counter indicates the message is fresh, the message is accepted, A substitutes
$$k_{AB} := k' \ ,$$
and increments the current index of k_{AB} by one. If the message was encrypted to a different key than k', the message is rejected, node A abandons proposed key k' remembering that it tried to change k_{AB} to k' but failed. This situation occurs if B has not received any message with the proposed key k' and has proposed a key itself.
4. If the counter in the received message is older than the one stored by A, this indicates a replay attack — the adversary is trying to make A change the key using an old message (for instance a message sent by A itself). As before, A should reject the message and abandon proposed key k' remembering that

it tried to change the key to k' but failed. Note that in this situation it might be the case that B has accepted k', but A is unaware of it. Recording k' will enable to accept k' in this case (see the procedure below).

Case 2: A receives a message from B while not waiting for a reply as in Case 1

1. If A receives a message from B encrypted with a certain key k'', then it tries to decrypt it by brute force. Namely,
   - A checks if $k'' = k_{AB}$,
   - if not, A tries keys of the form $F(k_{AB}, i)$ for all $i \leq l$ (or $F(k_{AB}, i, t)$ in the variant of the protocol, where t is the current index of k_{AB}),
   - if none of those keys work, and if A has previously tried to change the key to k' but failed, A tries keys of the form $F(k', i)$ (or $F(k', i, t)$ in the variant of the protocol). This option is necessary for the case in which B has accepted a new key k' proposed by A, while A received some invalid message and, according to the protocol, reverted to k_{AB}.

   If a valid decryption key is found and the message is fresh, then A waits until an opportune time to send its reply encrypted to k''. If $k'' \neq k_{AB}$, then the current index is incremented by one and k_{AB} is set to k''. If the message can not be decrypted or is not fresh, it is discarded.
2. If A receives further messages encrypted to k'', it processes them normally.
3. When A wants to send a message to B, it encrypts it with key k''.

Protocol Properties For space limitations we skip here the analysis of protocol correctness (which is essentially the same as for [1]). As in case of the scheme from [1], our protocol has several advantages: there is no communication overhead due to evolution of keys, rate of key evolution is automatically controlled by traffic volume, capturing a node does not compromise other nodes' keys, the scheme scales to any number of nodes, it can be used with any predistribution scheme. Extra energy consumption also remains negligible as in [1], as the only substantial difference is the addition of the one-way function, which can be based on AES [8], and performed using the same coprocessor that handles AES encryption/decryption. Another important point is that if the adversary somehow breaks a pairwise key from some moment, but transmissions between these nodes are not constantly monitored, then after a while the broken key becomes worthless.

The most important point is that KEP offers an important advantage over the one described in [1] in the event of node compromise. Even if an adversary has been eavesdropping on communications of the node, and recording them, the key extracted after compromising the node cannot be used to decrypt any of the recorded messages, as it is impossible to reverse the function F.

Main Problem In case of the protocol from [1] it is obvious that starting from an arbitrary key one can reach any key in the keyspace in a quite short time. Moreover, probability distribution describing the chances to reach each key converges fast to the uniform distribution over the keyspace.

It is unclear whether these uniformity and reachability properties hold for our KEP protocol: function F is pseudorandom but fixed. For this reason, key divergence process can have certain peculiarities. Consider a directed graph $G = (K, E)$, where the set of vertices K is the keyspace, and an arc kk' is in E if it is possible to make transition from key k to k' using rule (1). Even if F is pseudorandom it is not clear whether G is strongly connected (due to some reasons analogous to the birthday paradox). If digraph G is not strongly connected, then it may happen that there is a small subgraph G' of G such that after entering G' it it is impossible to leave G' (so G' would be like a black hole). For such subgraphs G' time-memory tradeoff attack [9] becomes very effective and endangers all keys contained in G'. In particular, in this case it would be possible to reverse key evolution without reversing F. Similarly, it would be easier to find the current pairwise key after breaking an old key even if the intermediate transmissions have not been recorded. We show in a rigid mathematical way that this is not the case – under certain assumptions G is strongly connected and has a small diameter with high probability (depending on the choice of F). This result would be much easier to obtain for rule (2). However, we concentrate on a mathematically hard case of rule (1) which is more elegant and easier to implement. For undirected random graphs connectivity and the diameter length were already widely studied, see for example B. Bollobás [10, 11] F. Chung and L. Lu [12]. Unfortunately those results can not be translated directly to the case of the directed graph model. Let us also remark that from combinatorial point of view connectivity for directed and undirected graphs are quite different issues.

Due to attacks like exhaustive search another property of key evolution is necessary. Namely, we have to show that there no "attractors", that is, the keys that are relatively often "visited" during key divergence process. If probability of visiting certain attractors is sufficiently large, an adversary can perform exhaustive search confined to the set of attractors. In such a way time complexity can be reduced considerably, while success probability might be still acceptable. We show that for rule (2) there are no attractors. Moreover, we show that probability distribution of a pairwise key is very close to uniform distribution after a small number of steps. By "similarity" we mean here a very strong measure of distance between probability distributions (much stronger than usually considered in papers on anonymous communication). Such a result for rule (1) is related to mixing time for directed graphs. However, known results concern undirected expander graphs [13]. Recent results were achieved for random graphs as well, but only undirected ones, or special forms of directed deterministic graphs [14–16]. These results are not applicable to our case. Moreover, our results are not asymptotic and apply in the case of relatively small graphs (on order of 2^{32}–2^{64} nodes).

Due to size limitation, we had to skip some details in the proof that we think can be reconstructed by a reader.

3 Key reachability – random digraph model

Preliminaries In this section we consider directed graph $G = (K, E)$, where the set of vertices K is the keyspace, and an arc kk' is in E if it is possible to make transition from key k to k' in one step of KEP according to rule (1). Let $K = \{0, 1\}^n$ and $N = 2^n$ denote the size of K.

We assume that the one-way function F changes a key into one of l keys, picked independently, uniformly at random. As there is a possibility of a collision, the actual number of possible keys in every step and for any initial key is a random variable X strongly concentrated around l. So, more generally, we consider the model of the random digraph $G(X) = (K, E)$ introduced in [17] (see also [18]) which is constructed in the following way:

- each vertex v chooses its out-degree l_v according to the distribution of $X_v = X$ independently of all other vertices,
- then, also independently of all other vertices, it chooses the set of l_v out–neighbors uniformly from all l_v-element subsets of K.

In this section, for a graph $G(X)$ defined by X such that $\mathrm{E}(X) \geq \ln N$ and X is concentrated around the expected value we shall formalize and find the lower bound on the probability that:

- $G(X)$ is strongly connected. This means, in the context of KEP protocol, that every key can eventually be transformed into every other key and there are no isolated groups of keys.

- The diameter of $G(X)$ is concentrated around $\frac{\ln N}{\ln l}$. So, any two keys can be transformed quickly into one another.

Let $d(u,v)=k$ mean that the shortest directed path from u to v has length k. Let us denote:

$$\varGamma_k^+(v) := \{w \in K : d(v,w)=k\}\ , \quad \varGamma_k^-(v) := \{w \in K : d(w,v)=k\}\ ,$$

$$N_k^+(v) := \bigcup_{i=0}^{k} \varGamma_i^+(v)\ , \quad N_i^-(v) := \bigcup_{i=0}^{k} \varGamma_i^-(v)\ , \quad \text{diam}G := \max\{d(u,v) : u, v \text{ are connected by a path}\}.$$

Since the the proofs include many estimations, and are rather technical, we will present sketches saving the exact calculations for the appendix. For clarity of calculations, we also make an assumption that $\frac{l}{2} \le X \le 2l$, which need not always be true in KEP. See Corollary 1 for remarks on a more general model.

Lemma 1 *Let X be a random variable such that $E(X)=l$ and $\Pr(\frac{l}{2} \le X \le 2l)=1$. In a graph $G(X)$ let A and B be disjoint subsets of K. If P_{AB} is the probability that v has an out–neighbor in A conditioned by the event that v has no out–neighbor in B, then for $N-|A|-|B| \ge \frac{l}{2}$*

$$\frac{l|A|}{N-|B|} - \frac{l^2|A|^2}{(N-|B|)^2} \le P_{AB} \le \frac{l|A|}{N-|B|} + \frac{l^2|A|}{(N-|B|)(N-|B|-2l)}. \tag{3}$$

Furthermore, if Y is a random variable counting those vertices in $K \setminus (A \cup B)$, which have out-neighbors in A, under the assumption that they do not have out–neighbors in B, then Y is binomially distributed with parameters $N-|A|-|B|$ and P_{AB}.

Proof. See appendix.

Theorem 1 *Let X be a random variable such that $E(X)=l$. If $\Pr(\lceil\frac{l}{2}\rceil \le X \le 2l)=1$, $N \ge 2^{32}$ and $\ln N \le l \le \sqrt{N}/90-1$, then with probability at least $1-p(N)$*

$$\lfloor \ln N/\ln 2l \rfloor \quad \le \quad \text{diam}\, G(X) \quad \le \quad \lceil \ln N/(2\ln\lfloor l/2\rfloor)\rceil + \lceil \ln N/(2\ln(\lceil l/2\rceil - 4))\rceil + 4\ ,$$

where: $p(N) = \frac{0.1(\ln N)^6}{N} + \frac{0.0017(\ln N)^{15}}{N^{1.99}} + \frac{1}{N^{0.59}} + \frac{1}{N^{0.16l}-1} + \frac{1}{N^{0.5}}$

In the proof we will frequently use simple probabilistic fact that if events H_1 and H_2 occur with probability at least $1-r_1$ and $1-r_2$ respectively and event H_3 conditioned on H_1 occurs with probability at least $1-r_3$, then
$\Pr(H_1 \cap H_2) = \Pr(H_1) + \Pr(H_2) - \Pr(H_1 \cup H_2) \ge 1 - r_1 - r_2$ and
$\Pr(H_1 \cap H_3) = \Pr(H_3|H_1)\Pr(H_1) \ge (1-r_1)(1-r_3) \ge 1 - r_1 - r_3$.

Proof (Sketch). To indicate the upper bound we will prove that with probability at least $1-p(N)$ if there exists a path between two vertices, then the shortest one has length at most $\left\lceil \frac{\ln N}{2\ln\lfloor\frac{l}{2}\rfloor} \right\rceil + \left\lceil \frac{\ln N}{2\ln(\lceil\frac{l}{2}\rceil-4)} \right\rceil + 4$. Namely, for vertices v_1 and v_2 we will estimate the number of vertices in $\varGamma_{k_1}^+(v_1)$ and in $\varGamma_{k_2}^-(v_2)$. Then we will prove that with probability close to one either these sets intersect, or there is an edge pointing from $\varGamma_{k_1}^+(v)$ to $\varGamma_{k_2}^-(w)$ for k_1+k_2+1 at most $\left\lceil \frac{\ln N}{2\ln\lfloor\frac{l}{2}\rfloor} \right\rceil + \left\lceil \frac{\ln N}{2\ln(\lceil\frac{l}{2}\rceil-4)} \right\rceil + 4$. To prove the lower bound on $\text{diam}G(X)$ we will estimate the size of $N_k^+(v)$. In fact we will show that for any vertex v there are some vertices at distance larger than $\left\lfloor \frac{\ln N}{\ln 2l} \right\rfloor$ from v.

First, for a given vertex $v \in K$, we will be considering sets of out–neighbors. Let us consider the process of labeling vertices, starting in vertex v. After this process, the set of vertices with label i will be the set $\varGamma_i^+(v)$. First, we will label vertex v with label 0. Then we will proceed one by one from $i = 0$. For given i if $\{w_1, w_2, \ldots, w_t\}$ are vertices with label i, then w_1 first labels all its out-neighbors, which were not labeled before, with label $i+1$. Then w_2 labels its out-neighbors in the same way, and so on. We will keep going as long as the set of vertices with label $i+1$ is smaller than $\sqrt{N}$.

Let $W = W(v)$ be a set of vertices labeled during the process and $A^v(w)$ be the event that during the process vertex $w \in W$ labels at least $\lceil \frac{l}{2} \rceil - 4$ vertices. If event $A^v = \bigcap_{w \in W} A^v(w)$ occurs, then each vertex with label i labels at least $\lceil \frac{l}{2} \rceil - 4$ vertices. Thus, $|\varGamma_{i+1}^+(v)| \geq \left(\lceil \frac{l}{2} \rceil - 4\right) |\varGamma_i^+(v)|$ and $|\varGamma_i^+(v)| \geq (\lceil \frac{l}{2} \rceil - 4)^i$ for all i. Therefore, if A^v occurs, then the process will stop in at most $k' = \frac{1}{2} \frac{\ln N}{\ln(\lceil \frac{l}{2} \rceil - 4)}$ steps (since $(\lceil \frac{l}{2} \rceil - 4)^{k'} \geq \sqrt{N}$) thus there exists an index $k_1(v) = k_1 \leq k'$ such that $|\varGamma_{k_1}^+(v)| \geq \sqrt{N}$.

Then, using estimations on $\Pr(\overline{\overline{A^v(w)}})$ (where $\overline{\overline{A^v(w)}}$ is the complement of event $A^v(w)$), we can prove (see Appendix) that for $N \geq 2^{32}$

$$\Pr\left(\forall_{v \in K} \exists_{0 \leq k_1(v) \leq k'} |\varGamma_{k_1(v)}^+(v)| \geq \sqrt{N}\right) \geq \Pr\left(\bigcap_{v \in K} A^v\right) \geq 1 - \Pr\left(\bigcup_{v \in K} \bigcup_{w \in W(v)} \overline{\overline{A^v(w)}}\right) \geq$$
$$\geq 1 - \sum_{v \in K} \sum_{w \in W(v)} \Pr\left(\overline{\overline{A^v(w)}}\right) \geq 1 - p_1(N), \tag{4}$$

where $p_1(N) = 0.1 \cdot (\ln N)^6 / N$.

Now we will estimate the sizes of sets of in–neighbors. Consider a vertex $v \in V$ such that v has at least two in–neighbors $u_1 \neq v$ and $u_2 \neq v$ or v has in–neighbor $u_1 \neq v$ which has in–neighbor $u_2 \neq v, u_1$. We will call such vertex v a “good” vertex. For a “good” vertex v, using Lemma 1 and the pigeonhole principle, we can prove (see Appendix) that with probability at least $1 - q_1(N)$ (where $q_1(N) = 0.0017 \cdot \frac{(\ln N)^{15}}{N^{2.99}}$) there exists i_0, $1 \leq i_0 \leq 3$, such that

$$|\varGamma_{i_0}^-(v)| \geq 6. \tag{5}$$

From now on, we assume that v is “good”. Let $k'' = \left\lceil \frac{1}{2} \frac{\ln N}{\ln \lfloor l/2 \rfloor} \right\rceil + 3$.

For all $0 < j \leq k''$ let:

– $B_j(v) = B_j$ be the event that $|\varGamma_j^-(v)| \geq 3\sqrt{N}$.

For all $i_0 < j \leq k''$ let:

– $C_j(v) = C_j$ be the event that $3 \left\lfloor \frac{l}{2} \right\rfloor^{j - i_0} \leq |\varGamma_j^-(v)| < 3\sqrt{N}$,

– $D_j(v) = D_j$ be the event that $|\varGamma_j^-(v)| \leq 3 \left\lfloor \frac{l}{2} \right\rfloor^{j - i_0}$.

Also denote by:

– $C_{i_0}(v)$ the event that $6 \leq |\varGamma_j^-(v)| < 3\sqrt{N}$,

– $D_{i_0}(v)$ the event that $|\varGamma_j^-(v)| < 6$.

Notice that by (5) we get:

$$\Pr(D_{i_0}) \leq q_1(N). \tag{6}$$

We will find a lower bound on the probability of the event $\bigcup_{i=0}^{k''} B_i$. Notice that if $\varOmega$ is the whole probability space, than for all $i_0 \leq i \leq k''$, we have $B_i \cup C_i \cup D_i = \varOmega$. Thus

$$\varOmega = B_{i_0} \cup (C_{i_0} \cap \varOmega) \cup D_{i_0} = B_{i_0} \cup (C_{i_0} \cap B_{i_0+1}) \cup D_{i_0} \cup (C_{i_0} \cap D_{i_0+1}) \cup (C_{i_0} \cap C_{i_0+1}) =$$
$$= \ldots = B_{i_0} \cup \bigcup_{i=i_0}^{k''-1} \left(B_{i+1} \cap \left(\bigcap_{j=i_0}^{i} C_j\right)\right) \cup D_{i_0} \cup \bigcup_{i=i_0}^{k''-1} \left(D_{i+1} \cap \left(\bigcap_{j=i_0}^{i} C_j\right)\right) \cup \left(\bigcap_{j=i_0}^{k''} C_j\right).$$

Also, by definition, $\bigcap_{j=i_0}^{k''} C_j = \emptyset$ since $3\sqrt{N} \le 3 \left\lfloor \frac{l}{2} \right\rfloor^{k''-i_0}$. Thus

$$\bigcup_{i=i_0}^{k''} B_i \supseteq B_{i_0} \cup \bigcup_{i=i_0}^{k''-1} \Big(B_{i+1} \cap \Big(\bigcap_{j=i_0}^{k''} C_j \Big) \Big) \cup \Big(\bigcap_{j=i_0}^{k''} C_j \Big).$$

Using Lemma 1 and Chernoff inequality we can prove that

$$\Pr(D_{i_0+1} \cap C_{i_0}) \le \left(\frac{1}{N}\right)^{1.59} \text{ and } \Pr\Big(D_{i+1} \cap \bigcap_{j=i_0}^{i} C_j\Big) \le \left(\frac{1}{N}\right)^{0.33 \cdot 0.5^{i-i_0}} \qquad (7)$$

for $i_0 + 1 \le i \le k'' - 1$. Thus from (6) and (7)

$$\begin{aligned} \Pr\Big(\bigcup_{i=0}^{k''} B_i(v)\Big) &\ge 1 - \Pr(D_{i_0}) - \sum_{i=i_0}^{k''-1} \Pr\Big(D_{i+1} \cap \bigcap_{j=i_0}^{i} C_j\Big) \ge \\ &\ge 1 - q_1(N) - \left(\frac{1}{N}\right)^{1.59} - \sum_{i=i_0+1}^{k''-2} \left(\frac{1}{N}\right)^{0.33\left(\frac{l}{2}\right)^{i-i_0}} \ge 1 - q_2(N), \end{aligned} \qquad (8)$$

where $q_2(N) = 0.0017(\ln N)^{15}/N^{2.99} + 1/N^{1.59} + 1/(N^{0.16l} - 1)$.
Assume that $\bigcup_{i=i_0}^{k''} B_i$ holds. Then there exists such k that $|\mathit{\Gamma}_k^-(v)| \ge 3\sqrt{N}$. Let $k_2 = k_2(v)$ be the smallest such index k. Using Lemma 1 and Chernoff inequality we can prove that

$$\Pr(|\mathit{\Gamma}_{k_2(v)}^-(v)| \ge 10\sqrt{N}) \le 1/N^{1.5}. \qquad (9)$$

Thus from (8) and (9)

$$\begin{aligned} &\Pr\left(\forall_{v \in K, v \text{ is ``good''}} \exists_{1 \le k_2 \le k''} 3\sqrt{N} \le |\mathit{\Gamma}_{k_2(v)}^-(v)| \le 10\sqrt{N}\right) \ge \\ &\ge 1 - \sum_{v \in K} \left(1 - \Pr\left(\exists_{1 \le k_2 \le k''} 3\sqrt{N} \le |\mathit{\Gamma}_{k_2(v)}^-(v)| \le 10\sqrt{N}\right)\right) \ge 1 - p_2(N), \end{aligned} \qquad (10)$$

where $p_2 = N\left(q_2 + 1/N^{1.5}\right)$.

From now on we will assume that v_1 and v_2 are the vertices such that

$$\exists_{1 \le k_1 \le k', 1 \le k_2 \le k''} |\mathit{\Gamma}_{k_1(v)}^+(v)| \ge \sqrt{N} \text{ and } 3\sqrt{N} \le |\mathit{\Gamma}_{k_1(v)}^+(v)| \le 10\sqrt{N} \qquad (11)$$

holds. We will find a lower bound on the probability that these vertices are connected by a directed path of length at most $k_1 + k_2 + 1$. If $\mathit{\Gamma}_{k_1}^+(v_1) \cap \mathit{\Gamma}_{k_2}^-(v_2) \neq \emptyset$, then there exists such a path. Otherwise, using Lemma 1, we may prove that the probability that there is an edge pointing from $\mathit{\Gamma}_{k_1}^+(v_1)$ to $\mathit{\Gamma}_{k_2}^-(v_2)$ is at least $1 - N^{\frac{3}{8}}$. Since there are at most N^2 pairs of vertices, thus with probability at least $1 - p_3(N)$ (where $p_3(N) = 1/N^{\frac{2}{3}}$) all pairs, for which (11) is fulfilled, are connected by a path of length at most $k' + k'' + 1$.

Concluding, since for any two vertices v_1 and v_2, such that v_2 is "good", (11) is fulfilled with probability at least $1 - p_1(N) - p_2(N)$, and so any pair of such vertices is connected by a directed path of length at most $k' + k'' + 1$ with probability at least $1 - p_1(N) - p_2(N) - p_3(N)$. Therefore, with probability at least $1 - p_1(N) - p_2(N) - p_3(N)$

$$\operatorname{diam} G(X) \le \lceil \ln N / (2 \ln \lfloor l/2 \rfloor \rceil + \lceil \ln N / (2 \ln(\lceil l/2 \rceil - 4)) \rceil + 4\ .$$

Furthermore, if $k''' = \left\lfloor \frac{\ln N}{\ln(2l)} \right\rfloor - 1$, then $|N^{+}_{k'''}(v)| \leq \sum_{i=0}^{k'''} (2l)^i = \frac{(2l)^{k'''+1}-1}{2l-1} \leq \frac{N-1}{2l-1} < N$. Thus, there exists a vertex $w \in K \setminus N^{+}_{k}(v)$. So diam $G(X) \geq k+1 = \left\lfloor \frac{\ln N}{\ln(2l)} \right\rfloor$.

Substituting $p(N) = p_1(N) + p_2(N) + p_3(N)$ finishes the proof.

□

Theorem 2 *Let X be a random variable such that* $E(X) = l \geq \ln N$ *and* $\Pr(\frac{l}{2} \leq X \leq 2l) = 1$. *If* $N \geq 2^{32}$ *and* $\ln N \leq l \leq \sqrt{N}/90 - 1$ *then*

the graph $G(X)$ *is strongly connected with probability at least* $1 - p'(N,l)$,

where $p'(N,l) = \frac{l}{N} \cdot \frac{N-l}{(N-2l)} \exp\left(\frac{2l(2l+1)}{N}\right) + N \exp\left(-l \cdot \frac{N-l-1}{N}\right) + \frac{0.1(\ln N)^6}{N} + \frac{0.0017(\ln N)^{15}}{N^{1.99}} + \frac{1}{N^{0.59}} + \frac{1}{N^{0.16l}-1} + \frac{1}{N^{0.5}}$

Proof (Sketch). Now, we shall estimate the probability that for any two vertices $v, w \in K$, there exists a directed (w,v)-path. We will find the lower bound on probability that any vertex in K is "good". Let $v \in K$. Substitute in Lemma 1 for $A = \{v\}$ and $B = \emptyset$, then v does not have any in–neighbor in $K \setminus \{v\}$ with probability:

$$(1 - P_{AB})^{N-1} \leq \exp(-P_{AB}(N-1)) \leq p'_1(N,l), \tag{12}$$

where $p'_1(N,l) = \exp\left(-l \cdot \frac{N-l-1}{N}\right)$. Moreover, using Lemma 1, we can estimate the probability that v has in–neighbor u but there is no vertex which would be in–neighbor of v or u by

$$\sum_{u \in K \setminus \{v\}} (1 - P_{\{v,u\},\emptyset})^{N-2} \cdot P_{\{v\},\emptyset} \leq p'_2(N,l), \tag{13}$$

where $p'_2(N,l) = \frac{l}{N^2} \cdot \frac{N-l}{(N-2l)} \exp\left(\frac{2l(2l+1)}{N}\right)$. Thus

$$\Pr(\exists_{v \in K} v \text{ is not "good"}) \leq \sum_{v \in K} \Pr(v \text{ is not "good"}) \leq N(p'_1(l,N) + p'_2(l,N)).$$

From the proof of Theorem 1, we know that in the graph $G(X)$ any two vertices $v_1, v_2 \in K$, such that v_2 is "good", are connected by a directed path from v_1 to v_2 with probability at least $1 - p(N)$. Moreover, with probability at least $1 - N(p'_1(l,N) + p'_2(l,N))$ each vertex in $G(X)$ is "good". Thus with probability at least $1 - p(N) - N(p'_1(l,N) - p'_2(l,N))$ graph $G(X)$ is connected.

Corollary 1 *(a) For* $N = 2^{32}$ *and* $l = 32 \geq \ln N$ *with probability larger than* 0.98*, graph* $G(X)$ *is connected and* $5 \leq$ *diam*$(G(X)) \leq 13$.
(b) For $N = 2^{64}$ *and* $l = 64 \geq \ln N$ *with probability larger than* $1 - \frac{3}{10^9}$*, graph* $G(X)$ *is connected and* $9 \leq$ *diam*$(G(X)) \leq 19$.
(c) If $\Pr(\frac{l}{2} \leq X \leq 2l) = 1 - p$*, then in graph* $G(X)$ *with probability at least* $1 - Np$ *for all vertices* $v \in K$ *we have* $\frac{l}{2} \leq X_v \leq 2l$*. Thus with probability at least* $1 - p'(l,N) - Np$ *graph* $G(X)$ *is connected and has diameter as stated in Theorem 1.*

4 Equalizing probability distribution

Now we consider KEP with rule (2). We are interested in the state of a key for a pair of nodes after t random transitions executed for a given initial state. Here, we model one-way function $F(-,-,\tau)$ as random functions chosen independently for each τ. The state of the key is a random variable with values that are keys reachable from the initial key in t steps. The corresponding probability distribution can be described as a vector $P^t = (P^t_1, P^t_2 \dots P^t_N)$, assuming that for all non-reachable keys we have 0 in this vector. Clearly, this vector depends on function F. The main issue is that certain keys can be reached in multiple ways and, consequently, the corresponding coordinates P^t_i might be significantly higher.

While in the previous section we have been interested in how many steps are necessary so that we can potentially reach every key, now our goal is to put an upper bound for deviation of the coordinate P^t_i from $1/N$ (corresponding to the uniform distribution on the keyspace) that holds for almost all transition functions.

In order to model the behavior of the key transition mechanism we analyze a stochastic process $\mathcal{B}$ expressed in terms of balls and bins. Let us consider N distinct bins and a single ball put in the first bin at the beginning of the process, i.e. for $t = 0$. At each step of the protocol each bin is linked to exactly $l \geq 2$ distinct bins chosen uniformly at random out of the set of all N bins. We demand that the connections chosen for bin i at round t are stochastically independent of the connections chosen for bin j at round t, for $i \neq j$, and that the connections in round t are independent of the connections in the previous rounds.

N bins correspond to all possible keys. The location of a ball indicates the current state of the considered key, l connections from the current bin to other bins correspond to possible key transitions. In order to simplify the considerations we assume that the number of keys that can be reached in one transition is exactly l, despite a small collision probability of a one-way function.

If the ball is in a particular bin at step t, it can be moved with equal probability to each of l bins at step $t+1$ linked to the bin holding the ball. Assume that for a given number of rounds, we fix the transitions. At time $t = 0$, we place the ball in the first bin. Then, for $t = 1$, it can be placed in each of l bins connected to the first bin with probability $1/l$. For $t = 2$, the potential number of reachable bins is within the interval $[l, l^2]$. Note that if a bin can be reached in multiple ways, then generally probability of placing the ball in it is higher. After a number of steps the situation becomes highly complex; the probabilities depend very much on the connections.

The Result Assuming the randomness of the transitions, P^t_i becomes a random variable. (Recall that for a given realization of connections P^t_i is simply the probability that in step t of process $\mathcal{B}$ the ball is in bin i.)

Theorem 3 *For step t of process $\mathcal{B}$ described above, with parameters $N > l \geq 2$, for $\varepsilon > 0$, and $\delta = \frac{1}{l} - \frac{1}{N}$ we have:*

$$\Pr\left(\max_i \left|P^t_i - \tfrac{1}{N}\right| \geq \varepsilon\right) \leq \left(\delta^t + \tfrac{\delta(1-\delta^{t-1})}{N(1-\delta)}\right)\varepsilon^{-2} .$$

Proof of Theorem 3 In the proof we consider the deviation of random vector P^t from the uniform distribution in terms of the random variable $\mathcal{D}_N(P^t)$:

$$\mathcal{D}_N(P^t) = \sum_{i=1}^N \left(P^t_i - \tfrac{1}{N}\right)^2 .$$

The proof is based on observations regarding the rate of decrease of the expectation of $\mathcal{D}_N(P^t)$ and finding a t such that this distance is close to zero. Since random variables P^{t+1}_i have the same distribution for each i, we get:

$$\mathrm{E}\left(\mathcal{D}_N(P^{t+1})|P^t\right) = \mathrm{E}\left(\left(P^{t+1}_1 - \tfrac{1}{N}\right)^2 + \ldots + \left(P^{t+1}_N - \tfrac{1}{N}\right)^2 \middle| P^t\right) = N \cdot \mathrm{E}\left(\left(P^{t+1}_1 - \tfrac{1}{N}\right)^2 \middle| P^t\right) .$$

Let $\phi(i, j, t)$ be a random variable describing the connection in round t, defined as follows: $\phi(i, j, t) = 1$ if bin i is linked to bin j at step t. Otherwise $\phi(i, j, t) = 0$.

Obviously, $\mathrm{E}\left(\phi(i,j,t)\right) = \frac{l}{N}$. Moreover, according to our assumptions the random variables $\phi(i_0, j_0, t_0)$ and $\phi(i_1, j_1, t_1)$ are independent if $i_0 \neq i_1$ or $t_0 \neq t_1$. By the above definition,

$$\mathrm{E}\Big(\Big(P_1^{t+1} - \tfrac{1}{N}\Big)^2 \Big| P^t\Big) = \mathrm{E}\Big(\Big(\textstyle\sum_i \frac{1}{l} \cdot P_i^t \cdot \phi(i,1,t) - \frac{1}{N}\Big)^2 \Big| P^t\Big) \ .$$

Since $\phi(i,1,t)$ and $\phi(j,1,t)$ are independent of P^t, we get

$$\mathrm{E}\left(\mathcal{D}_N(P^{t+1})|P^t\right) = N \cdot \mathrm{E}\Big(\Big(\sum_i \frac{1}{l} P_i^t \cdot \phi(i,1,t) - \frac{1}{N}\Big)^2 \Big| \, P^t\Big) =$$

$$= N \cdot \mathrm{E}\Big(\Big(\sum_i \frac{1}{l} \cdot P_i^t \cdot \phi(i,1,t) - \sum_i \frac{1}{l} \cdot P_i^t \cdot \frac{l}{N}\Big)^2 \Big| P^t\Big) = N \cdot \mathrm{E}\Big(\Big(\sum_i \frac{1}{l} \cdot P_i^t \cdot \Big(\phi(i,1,t) - \frac{l}{N}\Big)\Big)^2 \Big| P^t\Big) =$$

$$= N \sum_i \frac{1}{l^2} \cdot (P_i^t)^2 \cdot \mathrm{E}\Big(\Big(\phi(i,1,t) - \frac{l}{N}\Big)^2\Big) + N \sum_{i \neq j} \frac{1}{l^2} \cdot P_i^t \cdot P_j^t \cdot \mathrm{E}\Big(\Big(\phi(i,1,t) - \frac{l}{N}\Big) \cdot \Big(\phi(j,1,t) - \frac{l}{N}\Big)\Big) \ .$$

Let us note that $\phi(i,1,t)$ and $\phi(j,1,t)$ are independent for $i \neq j$. Since $\mathrm{E}(\phi(j,1,t)) = l/N$, the second sum is equal to 0. Moreover, $\mathrm{Var}(\phi(i,1,t)) = l/N \cdot (1 - l/N)$, so

$$\begin{aligned}
\mathrm{E}\left(\mathcal{D}_N(P^{t+1})|P^t\right) &= N \textstyle\sum_i \frac{1}{l^2} \cdot (P_i^t)^2 \frac{l}{N} \cdot \left(1 - \frac{l}{N}\right) = \left(\frac{1}{l} - \frac{1}{N}\right) \sum_i (P_i^t)^2 \\
&= \left(\tfrac{1}{l} - \tfrac{1}{N}\right) \cdot \Big(\textstyle\sum_i \Big((P_i^t)^2 - \frac{2 \cdot P_i^t}{N} + \frac{1}{N^2}\Big) + 2 \cdot \sum_i \frac{P_i^t}{N} - \sum_i \frac{1}{N^2}\Big) = \\
&= \left(\tfrac{1}{l} - \tfrac{1}{N}\right) \Big(\textstyle\sum_i \left(P_i^t - \frac{1}{N}\right)^2 + \frac{1}{N}\Big) = \left(\frac{1}{l} - \frac{1}{N}\right) \cdot \left(\mathcal{D}_N(P^t) + \frac{1}{N}\right) \ .
\end{aligned}$$

Hence, we have shown

$$\mathrm{E}\left(\mathcal{D}_N(P^{t+1})|P^t\right) = \left(\tfrac{1}{l} - \tfrac{1}{N}\right) \cdot \left(\mathcal{D}_N(P^t) + \tfrac{1}{N}\right) \ .$$

Taking expectation of both sides of the above equality gives us:

$$\mathrm{E}\left(\mathcal{D}_N(P^{t+1})\right) = \left(\tfrac{1}{l} - \tfrac{1}{N}\right) \cdot \mathrm{E}\left(\mathcal{D}_N(P^t)\right) + \left(\tfrac{1}{l} - \tfrac{1}{N}\right) \cdot \tfrac{1}{N} \ .$$

Let $\delta = \frac{1}{l} - \frac{1}{N}$. It is easy to check that $\mathrm{E}\left(\mathcal{D}_N(P^1)\right) = \delta$. Therefore, solving the recursive relation we get:

$$\mathrm{E}\left(\mathcal{D}_N(P^t)\right) = \mathrm{E}(\mathcal{D}_N(P^1)) \cdot \delta^{t-1} + \frac{\delta}{N} \cdot \left(1 + \delta + \ldots + \delta^{t-2}\right) = \delta^t + \frac{\delta(1 - \delta^{t-1})}{N(1-\delta)} \ .$$

Since $\mathcal{D}_N(P^t)$ is nonnegative, we can apply Markov inequality:

$$\Pr\left(\mathcal{D}_N(P^t) \geq \varepsilon^2\right) \leq \mathrm{E}(\mathcal{D}_N(P^t))/\varepsilon^2$$

and get:

$$\Pr\left(\mathcal{D}_N(P^t) \geq \varepsilon^2\right) \leq \left(\delta^t + \frac{\delta(1 - \delta^{t-1})}{N(1-\delta)}\right) \varepsilon^{-2} \ .$$

Therefore,

$$\begin{aligned}
\Pr\Big(\max_i \Big|P_i^t - \frac{1}{N}\Big| \geq \varepsilon\Big) &\leq \Pr\Big(\sum_i \Big(P_i^t - \frac{1}{N}\Big)^2 \geq \varepsilon^2\Big) \\
&= \Pr\left(\mathcal{D}_N(P^t) \geq \varepsilon^2\right) \leq \Big(\delta^t + \frac{\delta(1 - \delta^{t-1})}{N(1-\delta)}\Big) \varepsilon^{-2} \ .
\end{aligned}$$

This concludes the proof of Theorem 3. □

From previous considerations we immediately obtain the following corollaries:

Corollary 2 *For $l = 2^{m_1}$ and $N = 2^{m_2}$*

$$\Pr\left(\max_i \left|P_i^t - \frac{1}{N}\right| \geq \varepsilon\right) < \left(\left(\frac{2^{m_2-m_1}-1}{2^{m_2}}\right)^t + \frac{2^{m_2-m_1}-1}{2^{2m_2}-2^{2m_2-m_1}+2^{m_2}}\right)\cdot\varepsilon^{-2}\ .$$

Corollary 3

$$\Pr\left(\max_i \left|P_i^t - \frac{1}{N}\right| \geq \varepsilon\right) < \left(\left(\frac{N-2}{2N}\right)^t + \frac{N-2}{N(N+2)}\right)\varepsilon^{-2}\ .$$

for $l = 2$. In particular, for $l = 2$ and $t = \log N$

$$\Pr\left(\max_i \left|P_i^t - \frac{1}{N}\right| \geq \varepsilon\right) < \left(\frac{2}{N}\right)\varepsilon^{-2}\ .$$

References

1. Ren, M., Tanmoy, K.D., Zhou, J.: Diverging keys in wireless sensor networks. In Katsikas, S.K., Lopez, J., Backes, M., Gritzalis, S., Preenel, B., eds.: Information Security. Volume 4176 of LNCS., Springer Verlag (2006) 257–269 ISSN: 0302-9743, ISBN: 3-540-38341-7.
2. Carman, D.W., Kruus, P.S., Matt, B.J.: Constraints and approaches for distributed sensor network security. Technical Report 00-010, NAI Labs, Cryptographic Technologies Group Trusted Information Systems, NAI Labs, The Security Research Division Network Associates, Inc. 3060 Washington Road (Rt. 97) Glenwood, MD 21738-9745 (2000)
3. Tiri, K., Hwang, D., Hodjat, A., Lai, B., Yang, S., Schaumont, P., Verbauwhede, I.: Aes-based cryptographic and biometric security coprocessor ic in 0.18-um cmos resistant to side-channel power analysis attacks. In: 2005 Symposia on VLSI Technology and Circuits. (June 2005) 216–219
4. Eschenauer, L., Gligor, V.D.: A key-management scheme for distributed sensor networks. In: CCS '02: Proceedings of the 9th ACM conference on Computer and communications security, New York, NY, USA, ACM Press (2002) 41–47
5. Chan, H., Perrig, A., Song, D.: Random key predistribution schemes for sensor networks. In: SP '03: Proceedings of the 2003 IEEE Symposium on Security and Privacy, Washington, DC, USA, IEEE Computer Society (2003) 197–213
6. Chan, H., Perrig, A.: Pike: Peer intermediaries for key establishment in sensor networks. In: The 24th Conference of the IEEE Communications Society (Infocom 2005). (March 2005)
7. Anderson, R., Chan, H., Perrig, A.: Key infection: Smart trust for smart dust. In: Proceedings of IEEE International Conference on Network Protocols (ICNP 2004). (October 2004)
8. Daemen, J., Rijmen, V.: Rijndael specification. NIST "AES Algorithm (Rijndael) Information" webpage (2001)
9. Hellman, M.E.: A cryptanalytic time-memory tradeoff. IEEE Trans. Inform. Theory **26** (July 1980) 401–406
10. Bollobás, B.: The diameter of random graphs. IEEE Trans. Inform. Theory **36** (1990) 285–288
11. Bollobás, B.: Random Graphs. Academic Press (1985)
12. Chung, F., Lu, L.: The diameter of sparse random graphs. Adv. in Appl. Math. **26**(4) (2001) 257–279
13. Aldous, D., Fill, J.A.: Reversible markov chains and random walks on graphs-chapter 9: A second look at general markov chains
14. Nachmias, A., Peres, Y.: Critical random graphs: diameter and mixing time (2007)
15. Benjamini, I., Kozma, G., Wormald, N.: The mixing time of the giant component of a random graph (2006)
16. Montenegro, R., Tetali, P.: Mathematical aspects of mixing times in markov chains. Found. Trends Theor. Comput. Sci. **1**(3) (2006) 237–354
17. Jaworski, J., Smit, I.: On a random digraph. Annals of Discrete Mathathematics **33** (1987) 111–127
18. Jaworski, J., Palka, Z.: Remarks on a general model of a random digraph. Ars Combinatoria **65** (2002) 135–144
19. Janson, S., Łuczak, T., Ruciński, A.: Random Graphs. Wiley (2001)

Appendix

Proof of Lemma 1.

Lemma 2 *Let A and B be disjoint subsets of K, and let P^s_{AB} be the probability that in a graph $G(X)$ a given vertex v with degree s has an out-neighbor in A, conditioned by the event that it does not have any out-neighbor in B. Then for $N - |A| - |B| \geq s$:*

$$\tfrac{s|A|}{N-|B|} - \tfrac{s^2|A|^2}{2(N-|B|)^2} \leq P^s_{AB} \leq \tfrac{s|A|}{N-|B|} + \tfrac{s^2|A|}{2(N-|B|)(N-|B|-s)}. \tag{14}$$

Proof. Assume that vertex v with degree s does not have any out-neighbor in B. Then the probability that it does not have any out-neighbor in A is equal to $\frac{\binom{N-|A|-|B|}{s}}{\binom{N-|B|}{s}}$. Substituting $k = N - |B|$ and $|A| = d$ we have:

$$\frac{\binom{N-|A|-|B|}{s}}{\binom{N-|B|}{s}} = \frac{\binom{k-d}{s}}{\binom{k}{s}} = \prod_{i=0}^{s-1}\left(1 - \frac{d}{k-i}\right).$$

Furthermore,

$$\begin{aligned}\prod_{i=0}^{s-1}\left(1 - \frac{d}{k-i}\right) \leq \left(1 - \frac{d}{k}\right)^s \leq 1 - \frac{sd}{k} + \binom{s}{2}\frac{d^2}{k^2} \leq 1 - \frac{sd}{k} + \frac{s^2d^2}{2k^2} = \\ = 1 - \frac{s|A|}{N-|B|} + \frac{s^2|A|^2}{2(N-|B|)^2}\end{aligned}$$

and

$$\begin{aligned}\prod_{i=0}^{s-1}\left(1 - \frac{d}{k-i}\right) \geq 1 - \sum_{i=0}^{s-1}\frac{d}{k-i} = 1 - \sum_{i=0}^{s-1}\left(\frac{d}{k-i} - \frac{d}{k}\right) - \frac{sd}{k} = \\ = 1 - \frac{sd}{k} - \sum_{i=0}^{s-1}\frac{di}{k(k-i)} \geq 1 - \frac{sd}{k} - \frac{d}{k(k-s)}\binom{s}{2} \geq 1 - \frac{sd}{k} - \frac{s^2d}{2k(k-s)} = \\ = 1 - \frac{s|A|}{N-|B|} - \frac{s^2|A|}{2(N-|B|)(N-|B|-s)}\end{aligned}$$

which implies (14).

Proof (of Lemma 1). Using Lemma 2, since $X < 2l$ with probability 1,

$$\begin{aligned}
P_{AB} &= \sum_{s=0}^{2l} P_{AB}^{s} \cdot \Pr(X=s) \leq \\
&\leq \sum_{s=0}^{2l} \frac{|A|s}{N-|B|} \Pr(X=s) + \sum_{s=0}^{2l} \frac{|A|}{2(N-|B|)} \cdot \frac{s^2}{(N-|B|-s)} \cdot \Pr(X=s) \leq \\
&\leq \frac{l|A|}{N-|B|} + 2l \cdot \frac{|A|}{2(N-|B|)\cdot(N-|B|-2l)} \sum s \Pr(X=s) = \\
&\leq \frac{l|A|}{N-|B|} + \frac{l^2|A|}{(N-|B|)(N-|B|-2l)}
\end{aligned}$$

$$\begin{aligned}
P_{AB} &= \sum_{s=0}^{2l} P_{AB}^{s} \cdot \Pr(X=s) \geq \\
&\geq \sum_{s=0}^{2l} \frac{|A|s}{N-|B|} \Pr(X=s) - \sum_{s=0}^{2l} \frac{|A|s^2}{2(N-|B|)^2} \cdot \Pr(X=s) \geq \\
&\geq \frac{l|A|}{N-|B|} - 2l \cdot \frac{|A|}{2(N-|B|)^2} \sum_{s=0}^{2l} s \Pr(X=s) \geq \\
&\geq \frac{l|A|}{N-|B|} - \frac{l^2|A|}{(N-|B|)^2}
\end{aligned}$$

Moreover each vertex in $K \setminus (A \cup B)$ chooses its out–neighbors independently, therefore Y has a binomial distribution with parameters $N-|A|-|B|$ and P_{AB}.

Upper bound on $\Pr(\overline{\overline{A^v(w)}})$.

Assume that w has degree $s \geq \lceil \frac{l}{2} \rceil$ in $G(X)$. Notice that for $N \geq 2^{32}$ the procedure mentioned in the proof will not label more than $N^{+} = k'\sqrt{N} \leq \frac{\ln N\sqrt{N}}{2\ln(\lceil \frac{l}{2} \rceil - 4)} \leq \frac{\ln N\sqrt{N}}{4}$ vertices. Thus, probability that w during procedure labels less than $\lceil \frac{l}{2} \rceil - 4$ vertices is smaller than probability that w has at most $\lceil \frac{l}{2} \rceil - 5$ out–neighbors in the set of unlabeled vertices.

$$\Pr((A^v(w))^c) = \sum_{j=0}^{\lceil \frac{l}{2} \rceil - 5} \frac{\binom{N-N^{+}}{i}\binom{N^{+}}{s-j}}{\binom{N}{s}} \leq \sum_{j=0}^{\lceil \frac{l}{2} \rceil - 5} \binom{s}{s-j} \left(\frac{N^{+}}{N}\right)^{s-j} \leq \sum_{j=0}^{\lceil \frac{l}{2} \rceil - 5} \left(\frac{se}{s-j}\right)^{s-j} \left(\frac{N^{+}}{N}\right)^{s-j} \leq$$

$$\leq \sum_{j=0}^{\lceil \frac{l}{2} \rceil - 5} e \left(\frac{N^{+}e}{N}\right)^{s-i} \leq e \left(\frac{N^{+}e}{N}\right)^{5} \sum_{j=0}^{\lceil \frac{l}{2} \rceil - 5} \left(\frac{N^{+}e}{N}\right)^{j} \leq e \left(\frac{e \ln N\sqrt{N}}{4N}\right)^{5} \frac{4N}{4N - e\ln N\sqrt{N}} = q_3(N),$$

where $g_3(N) = \frac{e^6}{2^{10}} \frac{(\ln N)^5}{N^{2.5}} \frac{4N}{4N - e\ln N\sqrt{N}}$.
Thus for $N \geq 2^{32}$

$$\sum_{v \in K} \sum_{w \in W(v)} \Pr(\overline{\overline{A^v(w)}}) \leq N \frac{\ln N\sqrt{N}}{4} q_3(N) \leq \frac{0.1 \cdot (\ln N)^6}{N}.$$

Proof of (5)**.**

Let v be a good vertex. Let Z be a random variable counting number of vertices in $K\backslash\{v_0, v_1, v_2\}$ having an out–neighbor in $\{v_0, v_1, v_2\}$. Thus $\sum_{i=1}^{3} |\mathit{\Gamma}_i^-(v)| - 2 \geq |Z|$. According to Lemma 1, for $A := \{v_2, v_1, v_0\}$ and $B = \emptyset$, Z has binomial distribution $\mathrm{Bin}\,(N-3, P_{AB})$. For those A,B since $\frac{l+1}{N} \leq \frac{\sqrt{N}}{90N} + \frac{1}{N} < \frac{1}{3 \cdot 2^{20}}$ we have $P_{AB} \leq \frac{3l}{N}\left(1 + \frac{l}{N-2l}\right) < \frac{3l}{N}\left(1 + \frac{3l}{N}\right) < \frac{3(2^{20}+1)}{2^{40}}$ and $(N-3)P_{AB} \geq (N-3)\left(\frac{3l}{N} - \frac{9l^2}{N}\right) \geq 3l\left(1 - \frac{3(l+1)}{N}\right) > 3\ln N \frac{2^{20}-1}{2^{20}}$.
Furthermore

$$\begin{aligned}
\Pr(Z \leq 15) &= \sum_{i=0}^{15} \binom{N-3}{i} P_{AB}^i (1-P_{AB})^{N-3-i} \leq \\
&\leq \sum_{i=0}^{15} \left(\frac{(N-3)P_{AB}e}{i}\right)^i \exp\left(-(N-3-i)P_{AB}\right) \leq \\
&\leq 16\exp(15P_{AB}) \left(\frac{(N-3)P_{AB}}{\frac{i}{e}}\right) \exp(-(N-3)P_{AB}) < \\
&< 16\exp\left(15\frac{3(2^{20}+1)}{2^{40}}\right) \left(\frac{3\ln N \frac{2^{20}-1}{2^{20}} e}{15}\right)^{15} \exp\left(-3\ln N \frac{2^{20}-1}{2^{20}}\right) < \\
&< 16\exp\left(15\frac{3(2^{20}+1)}{2^{40}}\right) \cdot (0.54 \cdot \ln N)^{15} \left(\frac{1}{N}\right)^{2.99} < 0.0017 \cdot \frac{(\ln N)^{15}}{N^{2.99}} = q_1(N),
\end{aligned}$$

since the function $f(x) = x^i \exp(-x)$ is decreasing for $x > i$ and the function $f(x) = \frac{a^x}{x^x}$ is increasing for $x < \frac{a}{e}$.
Therefore, for a "good" vertex v, $\sum_{i=1}^{3} |\mathit{\Gamma}_i^-(v)| - 2 \geq |Z| \geq 16$ with probability at least $1 - q_1(N)$, and thus by pigeonhole principle with probability at least $1 - q_1(N)$ there exists i_0, $1 \leq i_0 \leq 3$, such that

$$|\mathit{\Gamma}_{i_0}^-(v)| \geq 6, \tag{15}$$

which proves (5).

Proof of (7)

For any $i_0 < i \leq k'' = \left\lceil \frac{\ln N}{2\ln\lfloor\frac{l}{2}\rfloor} \right\rceil + 3$ and v – a "good" vertex we will find a lower bound on the size of $\mathit{\Gamma}_i^-(v)$. Notice that a set $\mathit{\Gamma}_{i+1}^-(v)$ consists of all vertices from $K \setminus (\mathit{\Gamma}_i^-(v) \cup N_{i-1}^-(v))$ having an out–neighbor in $\mathit{\Gamma}_i^-(v)$, thus by Lemma 1, if we assume that $|\mathit{\Gamma}_i^-(v)| = \mathit{\Gamma}$ and $|N_{i-1}^-(v)| = N_i$ we have:

$$|\mathit{\Gamma}_{i+1}^-(v)| \sim \mathrm{Bin}\left(N - N_i - \mathit{\Gamma}, P_{\mathit{\Gamma} N_i}\right), \tag{16}$$

and

$$\frac{\mathit{\Gamma} l}{N - N_i} - \frac{\mathit{\Gamma}^2 l^2}{(N - N_i)^2} \leq P_{\mathit{\Gamma} N_i}.$$

Furthermore if we condition that event $\bigcap_{j=i_0}^{i} C_j$ occurs, then: $3\left(\frac{l}{2}\right)^{i-i_0} \leq |\Gamma_i^-(v)| < 3\sqrt{N}$ and $|N_{i-1}^-(v)| \leq 3k''\sqrt{N}$. Moreover since $l \leq \frac{\sqrt{N}}{90} - 1$ for $\Gamma \leq 3\sqrt{N}$ and $N_i \leq (\frac{1}{2}\ln N + 3)\sqrt{N}$

$$\begin{aligned} E\Gamma_{i+1}^- &= (N - N_i - \Gamma)P_{\Gamma N_i} \geq \\ &\geq \Gamma l - \frac{\Gamma^2 l^2}{(N-N_i)} - \frac{\Gamma^2 l}{(N-N_i)} + \frac{\Gamma^3 l^2}{(N-N_i)^2} \geq \Gamma l \left(1 - \frac{\Gamma(l+1)}{(N-N_i)}\right) \geq a\Gamma l \end{aligned}$$

Where $a = \frac{28999}{30000}$.
By $F_i(\Gamma)$ we denote event that $\bigcap_{j=i_0}^{i} C_j$ and $\Gamma_i^-(v) = \Gamma$. Then by Chernoff inequality (see for example [19] theorem 2.1), for $i \geq i_0$

$$\begin{aligned} &\Pr(|\Gamma_{i+1}^-| \leq b\Gamma_i^- l | F_i(\Gamma)) = \\ &= \Pr\left(|\Gamma_{i+1}^-| \leq \frac{b}{a} E(|\Gamma_{i+1}^-||F_i(\Gamma))\middle| F_i(\Gamma)\right) \leq \\ &\leq \Pr\left(|\Gamma_{i+1}^-| \leq E(|\Gamma_{i+1}^-||F_i(\Gamma)) - \left(1 - \frac{b}{a}\right) E(|\Gamma_{i+1}^-||F_i(\Gamma))\middle| F_i(\Gamma)\right) \leq \\ &\leq \exp\left(-\frac{(1-\frac{b}{a})^2 (E(|\Gamma_{i+1}^-||F_i(\Gamma)))^2}{2E(|\Gamma_{i+1}^-||F_i(\Gamma))|}\right) \leq \exp\left(-\frac{(1-\frac{b}{a})^2}{2} a\Gamma l\right) \end{aligned} \tag{17}$$

Thus substituting $i = i_0$, $a = \frac{28999}{30000}$ and $b = 0.25$ for $6 \leq \Gamma \leq 3\sqrt{N}$:

$$\Pr(|\Gamma_{i_0+1}^-| \leq 0.25|\Gamma_{i_0}^-|l||\Gamma_{i_0}^-| = \Gamma) \leq \exp\left(-\frac{(1 - 0.25\frac{30000}{28999})^2}{2}\frac{28999}{30000}\Gamma l\right) \leq \left(\frac{1}{N}\right)^{1.59}.$$

Therefore since $0.25 \cdot 6 \cdot l \geq 3\left\lfloor \frac{l}{2} \right\rfloor$ thus:

$$\Pr(D_{i_0+1}|C_{i_0}) \leq \sum_{\Gamma=6}^{3\sqrt{N}} \Pr(\Gamma_{i+1}^- \leq 0.3\Gamma_{i_0}^- l | \Gamma_{i_0}^- = \Gamma) \leq \left(\frac{1}{N}\right)^{1.59}$$

and

$$\Pr(D_{i_0+1} \cap C_{i_0}) = \Pr(D_{i_0+1}|C_{i_0}) \Pr(C_{i_0}) \leq \left(\frac{1}{N}\right)^{1.59},$$

which is the first part of (7).
Furthermore for $i > i_0$ substituting $a = \frac{28999}{30000}$ and $b = \frac{1}{2}$ for $3\left\lfloor \frac{l}{2} \right\rfloor^{i-i_0} \leq \Gamma \leq 3\sqrt{N}$:

$$\Pr(|\Gamma_{i+1}^-| \leq \frac{1}{2}|\Gamma_i^-|l|F_i(\Gamma)) \leq \exp\left(-\frac{(1 - \frac{1}{2}\frac{30000}{28999})^2}{2}\frac{28999}{30000}\Gamma l\right) \leq \left(\frac{1}{N}\right)^{0.33\left(\frac{l}{2}\right)^{i-i_0}}.$$

Therefore since $\frac{1}{2} \cdot 3\left\lfloor \frac{l}{2} \right\rfloor^{i-i_0} \cdot l \geq 3\left\lfloor \frac{l}{2} \right\rfloor^{i+1-i_0}$ and $\bigcap_{j=i_0}^{i} C_j = \bigcup_{\Gamma=3\left(\frac{l}{2}\right)^{i-i_0}}^{3\sqrt{N}} F_i(\Gamma)$ thus

$$\Pr\left(D_{i+1}\middle| \bigcap_{j=i_0}^{i} C_j\right) \leq \frac{\sum_{\Gamma=3\left(\frac{l}{2}\right)^{i-i_0}}^{3\sqrt{N}} \Pr(|\Gamma_{i+1}^-| \leq \frac{1}{2}|\Gamma_i^-|l|F_i(\Gamma)) \Pr(F_i(\Gamma))}{\Pr\left(\bigcap_{j=i_0}^{i} C_j\right)} \leq \left(\frac{1}{N}\right)^{0.33\left\lfloor \frac{l}{2} \right\rfloor^{i-i_0}}$$

and

$$\Pr\left(D_{i+1} \cap \bigcap_{j=i_0}^{i} C_j\right) \leq \left(\frac{1}{N}\right)^{0.33\left\lfloor \frac{l}{2} \right\rfloor^{i-i_0}},$$

which is the second part of (7).

Proof of (9) – an upper bound on $\boldsymbol{\Gamma^-_{k_2}(v)}$

Assume that there exists $k_2 \leq k''$ - the smallest index such that $\Gamma^-_{k_2}(v)$ is larger then $3\sqrt{N}$. Thus $1 \leq |\Gamma^-_{k_2-1}(v)| \leq 3\sqrt{N}$ and $|N_{k_2-1}| \leq 3k''\sqrt{N}$. Since (16) holds thus from Lemma 1 we have

$$P_{\Gamma N_i} \leq \frac{\Gamma l}{N - N_i} + \frac{\Gamma l^2}{(N - N_i)(N - N_i - 2l)}$$

and

$$\begin{aligned} E|\Gamma^-_{i+1}| = (N - N_i - \Gamma)P_{\Gamma N_i} \leq (N - N_i)P_{\Gamma N_i} \leq \\ \leq \Gamma l\left(1 + \frac{l}{N - N_i - 2l}\right) \leq \Gamma l\left(1 + \frac{3l}{N - N_i}\right). \end{aligned}$$

Then by Chernoff bound for $1 \leq \Gamma \leq 3\sqrt{N}$ and $|N_{k_2-1}| \leq 3k''\sqrt{N}$:

$$\begin{aligned} \Pr(|\Gamma^-_{k_2}| \geq 10\sqrt{N} \| \Gamma^-_{k_2-1}| = \Gamma) &\leq \Pr\left(|\Gamma^-_{k_2}| \geq 3\Gamma l\left(1 + \frac{3l}{N - |N_{k_2-1}|}\right) \middle| |\Gamma^-_{k_2-1}| = \Gamma\right) \leq \\ &\leq \Pr\left(|\Gamma^-_{k_2}| \geq E(|\Gamma^-_{k_2}||\Gamma) + 2\Gamma l\left(1 + \frac{3l}{N - |N_{k_2-1}|}\right) \middle| |\Gamma^-_{k_2-1}| = \Gamma\right) \leq \\ &\leq \exp\left(-\frac{4\Gamma^2 l^2\left(1 + \frac{3l}{N - |N_{k_2-1}|}\right)^2}{2\left(E(|\Gamma^-_{k_2}||\Gamma) + \frac{1}{3}\Gamma l\left(1 + \frac{3l}{N - |N_{k_2-1}|}\right)\right)}\right) \leq \\ &\leq \exp\left(-\frac{3}{2}\Gamma l\left(1 + \frac{3l}{N - |N_{k_2-1}|}\right)\right) \leq \frac{1}{N^{\frac{3}{2}}} \end{aligned}$$

Thus conditioned on the fact that $1 \leq \Gamma \leq 3\sqrt{N}$ and $|N_{k_2-1}| \leq 3k''\sqrt{N}$ holds

$$\Pr(|\Gamma_{k_2}| \geq 10\sqrt{N}) \leq \sum_{\Gamma=1}^{3\sqrt{N}} \Pr(|\Gamma^-_{k_2}| \geq 10\sqrt{N} \| \Gamma^-_{k_2-1}| = \Gamma) \Pr(|\Gamma^-_{k_2-1}| = \Gamma) \leq N^{\frac{3}{2}},$$

which implies (9)

Existence of paths

From Lemma 1 substituting $A = \Gamma^-_{k_2}(v_2)$, and $B = \emptyset$ we know that the probability that vertex $u \in \Gamma^-_{k_2}(v_2)$ does not have any out-neighbor in $\Gamma^-_{k_2}(v_2)$ is equal to $1 - P_{AB}$. Thus for $\Gamma^+_{k_1}(v_1)$ and $\Gamma^-_{k_2}(v_2)$ such that

$|\varGamma^+_{k_1}(v_1)| \geq \sqrt{N}$ and $3\sqrt{N} \leq |\varGamma^-_{k_2}(v_2)| \leq 10\sqrt{N}$, since $l \leq \frac{\sqrt{N}}{90}$, the probability that there are no edges pointing from $\varGamma^+_{k_1}(v)$ to $\varGamma^-_{k_2}(w)$ is:

$$
\begin{aligned}
(1-P_{AB})^{|\varGamma^+_{k_1}|} &\leq \left(1 - \frac{|\varGamma^-_{k_2}|l}{N} + \frac{|\varGamma^-_{k_2}|^2 l^2}{N^2}\right)^{|\varGamma^+_{k_1}|} \leq \\
&\leq \exp\left(\left(-\frac{|\varGamma^-_{k_2}|l}{N} + \frac{|\varGamma^-_{k_2}|^2 l^2}{N^2}\right)|\varGamma^+_{k_1}|\right) \leq \\
&\leq \exp\left(-|\varGamma^-_{k_2}| \cdot |\varGamma^+_{k_1}| l \left(1 - \frac{|\varGamma^-_{k_2}|l}{N}\right)\right) \leq \left(\frac{1}{N}\right)^{3\left(1-\frac{|\varGamma^-_{k_2}|l}{N}\right)} \leq \frac{1}{N^{\frac{8}{3}}}.
\end{aligned}
$$

Proof of (12) **and** (13)

For $A = \{v\}$ and $B = \emptyset$ from Lemma 1

$$
\begin{aligned}
(1-P_{AB})^{N-1} &\leq \exp(-P_{AB}(N-1)) \leq \\
&\leq \exp\left(-(N-1)\cdot\frac{l}{N}(1-\frac{l}{N})\right) = \\
&= \exp\left(-\left(l\left(1-\frac{l}{N}\right) - \frac{l}{N}\left(1-\frac{1}{N}\right)\right)\right) = \\
&= \exp\left(-l\left(1 - \frac{l}{N} - \frac{1}{N} + \frac{l}{N^2}\right)\right) \leq \exp\left(-l\left(1-\frac{l+1}{N}\right)\right).
\end{aligned}
$$

Using Lemma 1 twice we have

$$
\begin{aligned}
&\sum_{v_1 \in K\setminus\{v\}} (1-P_{\{v,v_1\},\emptyset})^{N-2} \cdot P_{\{v\},\emptyset} \leq \\
&\leq (N-1)\cdot\left(1-\frac{2l}{N}+\frac{4l^2}{N^2}\right)^{N-2} \cdot \left(\frac{l}{N} + \frac{l^2}{N(N-2l)}\right) \leq \\
&\leq (N-1)\cdot\exp\left(-2l + \frac{2l}{N} + \frac{4l^2}{N} - \frac{8l^2}{N^2}\right)\cdot\left(\frac{l}{N} + \frac{l^2}{N(N-2l)}\right) \leq \\
&\leq (N-1)\cdot\frac{1}{N^2}\cdot\exp\left(\frac{2l}{N}+\frac{4l^2}{N}\right)\cdot\left(\frac{l}{N} + \frac{l^2}{N(N-2l)}\right) \leq \\
&\leq \exp\left(\frac{2l}{N}(1+2l)\right)\cdot\frac{l}{N^2}\left(1+\frac{l}{(N-2l)}\right).
\end{aligned}
$$