J. Appl. Math. & Informatics Vol. 26(2008), No. 3 - 4, pp. 563 - 572
Website: http://www.kcam.biz

GENERALIZATION OF KEY DISTRIBUTION PATTERNS FOR EVERY n-PAIR OF USERS

SEON HO SHIN* AND JULIA C. BATE

ABSTRACT. In this paper, we discuss about a generalization of the Key Distribution Pattern which was proposed by C. Mitchell and F. Piper[6]. It is allowing secure communication between every n-pair of users($n \geq 2$) in a large network for reducing storage requirements. We further suggest a generalization of K. Quinn's bounds in [9] for the number of subkeys in such general Key Distribution Patterns.

AMS Mathematics Subject Classification : 94C30, 05B30, 51E30
Key words and phrases : Finite incidence structures, key distribution patterns, combinatorial designs

1. Introduction

Key distribution scheme is one of the important problems in communication and network security. In 1988, C. Mitchell and F. Piper proposed the use of a certain special kind of finite incidence structure that is called a *Key Distribution Pattern*(simply KDP), in order to give an efficient solution to main key storage problem in key distribution scheme[6]. It provides a secure method of distributing keys between every pair of users in a large network reducing storage requirements.

The purpose of this paper is to generalize a concept of such KDP for every n-pair of users($n \geq 2$). We call this general KDP a G_n-*KDP*. In fact a G_n-KDP is more useful than the original KDP because it is applicable to every n-pair of users($n \geq 2$). In this case the key to be used by a n-pair of users to allow them to communicate secure is made up from those subkeys which the n-pair of users have in common.

First, we introduce some generalized equivalence properties of G_n-KDP for every n-pair of users and useful examples of these schemes. Using the property

Received November 23, 2007. *Corresponding author.
This work was supported by the Soongsil University Research Fund.

that a finite incidence structure $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is a G_n-KDP iff the internal structure of $\mathcal{K}$ at $P \in \mathcal{P}$ is a G_{n-1}-KDP, we show that $(n+1)$-(v, k, λ) design is a G_n-KDP. Also we show that an G_{n+1}-KDP is again a G_n-KDP, that is, G_{n+1}-KDP $\subset G_n$-KDP $\subset G_{n-1}$-KDP $\subset \cdots$ $(n \geq 2)$. In order to make up the maximal such n, we suggest a construction and have an example for it.

To consider such problem of collusion in G_n-KDP, we also provide some equivalence properties of G_n-KDP which is secure against collusion by up to some number w of users. Such a special G_n-KDP is called a G_n^w-*KDP* in this paper. For reference, it was called a (n, w)-*collusion resistant KDP* by C. Mitchell and F. Piper[6].

Next, we generalize K. Quinn's two lower bounds in [9] for the number of subkeys at each user in G_n^w-KDP. Two lower bounds we have are

$$w\{log_2(v-1)\cdots(v-n+1) - \log_2(n-1)! - \log_2 w\} \text{ and}$$
$$min\{v-1, \tfrac{1}{2}(w+n-1)(w+n)\}.$$

For the terminology not introduced in this paper, we refer to [5] for the design theory.

2. Key distribution patterns for every n-pair of users

Key Distribution Patterns are public patterns of subsets produced using finite incidence structures. A *finite incidence structure* is a triple $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, where $\mathcal{P}$ is a nonempty finite set of points, $\mathcal{B}$ is a nonempty finite set of blocks and $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$ is a binary relation between $\mathcal{P}$ and $\mathcal{B}$. If $(P, x) \in \mathcal{I}$, where $P \in \mathcal{P}$ and $x \in \mathcal{B}$, then we say that P *is incident with* x or x *is incident with* P. We denote the set of points incident with a block x by (x) and the set of blocks incident with a point P by (P).

First of all, we introduce some generalized equivalence properties for every pair of users as well as for every n-pair$(n \geq 3)$ of users .

Lemma 1. *Let $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a finite incidence structure with $|\mathcal{P}| \geq 3$. For $n \geq 2$, the following properties are equivalent.*

(1) *For any n points $P_1, P_2, \cdots, P_n \in \mathcal{P}$,*

$$\bigcap_{i=1}^{n}(P_i) \subset (P_m) \textit{ if and only if } P_i = P_m \textit{ for some } i.$$

(2) *The set* $\left\{\bigcap_{i=1}^{n}(P_i) : P_i(1 \leq i \leq n) \textit{ are all distinct points of } \mathcal{P}\right\}$ *is a Sperner system of subsets of $\mathcal{B}$, that is, for every $\bigcap_{i=1}^{n}(P_i)$ and $\bigcap_{j=1}^{n}(Q_j)$ in the above set such that $\bigcap_{i=1}^{n}(P_i) \subset \bigcap_{j=1}^{n}(Q_j)$, $\bigcap_{i=1}^{n}(P_i) = \bigcap_{j=1}^{n}(Q_j)$.*

(3) *Every line through distinct n points in $\mathcal{K}$ has size n, where a line through distinct n points $P_1, P_2, \cdots, P_n$ is the set of all points which are incident with every block in $\bigcap_{i=1}^{n}(P_i)$.*

(4) *For any* $n+1$ *distinct points* $P_1, P_2, \cdots, P_n$ *and* Q *of* $\mathcal{P}$,

$$\left|\bigcap_{i=1}^{n}(P_i)\backslash(Q)\right| \geq 1.$$

(5) *The set* $\left\{x_j : \{P_1, P_2, \cdots, P_n\} \subset x_j \text{ and } \{Q\} \cap x_j = \emptyset\right\}$ *is nonempty for all distinct points* $P_1, P_2, \cdots, P_n$ *and* Q.

Proof. Suppose that $\bigcap_{i=1}^{n}(P_i) \subset \bigcap_{j=1}^{n}(Q_j)$ for any P_i and Q_j in $\mathcal{P}(1 \leq i, j \leq n)$. Then $\bigcap_{i=1}^{n}(P_i) \subset (Q_j)$ for all j. By the assumption (1), $P_i = Q_j$ for some i and for all j. Hence $\bigcap_{i=1}^{n}(P_i) = \bigcap_{j=1}^{n}(Q_j)$, that is, the set

$$\left\{\bigcap_{i=1}^{n}(P_i) : P_i(1 \leq i \leq n) \text{ are all distinct elements of } \mathcal{P}\right\}$$

is a Sperner system of subsets of $\mathcal{B}$. Thus (1) implies (2).

Next, to show (2) implies (3), suppose that there exists a line through distinct n points in $\mathcal{P}$ which has no size n. Then there exist at least distinct $n+1$ points P_1, $P_2, \cdots, P_n$ and Q in $\mathcal{K}$ such that $\bigcap_{i=1}^{n}(P_i) \subset (Q)$. Hence $\bigcap_{i=1}^{n}(P_i) \subset (Q) \cap \bigcap_{i=1}^{n-1}(P_i)$. By (2), $\bigcap\limits_{i=1}^{n}(P_i) = (Q) \cap \bigcap\limits_{i=1}^{n-1}(P_i)$. Therefore $P_i = Q$ for some i, which is a contradiction.

To show (3) implies (4), suppose on the contrary that there exist $n+1$ distinct points P_1, $P_2, \cdots, P_n$ and Q in $\mathcal{P}$ such that

$$\left|\bigcap_{i=1}^{n}(P_i)\backslash(Q)\right| < 1, \text{ i.e., } \bigcap_{i=1}^{n}(P_i) \subset (Q).$$

Assume that $\bigcap_{i=1}^{n}(P_i) \neq \emptyset$. By (3), every line through distinct n points in $\mathcal{K}$ has size n, but the number of the set of all points which are incident with every block in $\bigcap_{i=1}^{n}(P_i)$ is greater than or equal $n+1$. It is a contradiction.

Since $\{P_1, P_2, \cdots, P_n\} \subset x_j$ and $\{Q\} \cap x_j = \emptyset$ mean that the block x_j is incident with n points $P_1, P_2, \cdots, P_n$ and is not incident with the point Q, the result of (5) from (4) follows immediately.

For the last implication, it is enough to consider the necessary condition. Suppose on the contrary that there are all distinct $n+1$ points $P_1, P_2, \cdots, P_n$ and Q in $\mathcal{P}$ such that $\bigcap_{i=1}^{n}(P_i) \subset (Q)$. Since there exists a block x_j such that is incident with n points $P_1, P_2, \cdots, P_n$ and is not incident with the point Q, we have an immediate contradiction and desired result follows. The proof is complete. □

We often identify each point of $\mathcal{K}$ as a *user* in the network and each block of $\mathcal{K}$ as a *subkey* between users. The key to be used by a n-pair of users to allow them to communicate securely is made up from those subkeys which the n-pair of users have in common.

Definition 1. A finite incidence structure $\mathcal{K}$ is called *a G_n-Key Distribution Pattern*(simply G_n-KDP)($n \geq 2$) if it is satisfied with one of the equivalent properties in Lemma 1.

We note that a G_2-KDP is precisely the same object as the original KDP by C. Mitchell and F. Piper. Also it is clear from the definition that $P_1, P_2, \cdots, P_{n-1}$ and P_n share at least one subkey not in the subkey set of distinct user Q from $P_1, P_2, \cdots, P_n$, that is, for any G_n-KDP, the key of any n-pair of users cannot be determined from the subkeys of any other users.

All of these similarities to KDPs ensure that G_n-KDPs inherit many interesting characteristics and retain the design theory notation of the original KDPs. We note that a G_n-KDP can be represented by a $v \times b$ incidence matrix $A = (a_{ij})$, where $v = |\mathcal{P}|$ and $b = |\mathcal{B}|$, which is defined as follows: $a_{ij} = 1$ if the user P_i is incident with the block x_j, and $a_{ij} = 0$ otherwise.

Example 1. (1) A n-$(v, n, 1)$ design is always a G_n-KDP. This is what we call the *trivial G_n-KDP*. Moreover, it is a nontrivial G_{n-1}-KDP(we have more detail for proof in Theorem 2).

(2) Some of 2-(v, k, λ) design and 3-(v, k, λ) design are G_2-KDPs(see [6,7]), for example, 2-$(5, 4, 3)$ design and 3-$(6, 5, 3)$ design are G_2-KDPs.

(3) Consider the following incidence matrix

$$A = (a_{ij}) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

If we label the rows as users $P_1, P_2, \cdots, P_5$ and the columns as subkeys $x_1, x_2, \cdots, x_8$, then A represents a non-trivial G_3-KDP.

(4) 3-$(5, 4, 2)$ design is a G_3-KDP.

Before considering any further examples we need some basic definitions in [5].

If $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is a finite incidence structure and $P \in \mathcal{P}$, then the *internal structure* $\mathcal{K}_P$ of $\mathcal{K}$ at P is defined by the structure having point set $\mathcal{P} \backslash \{P\}$ and block set $\{x \in \mathcal{B} : x \text{ contains } P\}$. Also the *external structure* $\mathcal{K}^P$ of $\mathcal{K}$ at P is defined by the structure having point set $\mathcal{P} \backslash \{P\}$ and block set $\{x \in \mathcal{B} : x \text{ does not contain } P\}$.

Lemma 2. *Let $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a finite incidence structure. Then $\mathcal{K}$ is a G_n-KDP if and only if the internal structure $\mathcal{K}_P$ of $\mathcal{K}$ is a G_{n-1}-KDP.*

Proof. For any user $P \in \mathcal{P}$ and any distinct n users $P_1, P_2, \cdots, P_{n-1}$ and Q in $\mathcal{K}_P$,

$$\left| \left[\bigcap_{i=1}^{n-1} (P_i) \cap (P) \right] \backslash (Q) \right| \geq 1$$

since $\mathcal{K}$ is a G_n-KDP. That is, there is a subkey incident with all $P_i (1 \leq i \leq n-1)$ and P but not incident with Q. Since $\bigcap_{i=1}^{n-1}(P_i) \cap (P) \subset \bigcap_{i=1}^{n-1}(P_i)$, $| \bigcap_{i=1}^{n-1}(P_i) \backslash (Q) | \geq 1$. Hence $\mathcal{K}_P$ is a G_{n-1}-KDP.

Conversely for any $P_1, P_2, \cdots, P_{n-1}, P$ and Q in $\mathcal{K}$, $\left| \bigcap_{i=1}^{n-1} (P_i) \backslash (Q) \right| \geq 1$, that is, there is a subkey which is incident with all $P_i (1 \leq i \leq n-1)$ but not incident with Q in $\mathcal{K}_P$. Since all blocks in $\mathcal{K}_P$ are incident with P,

$$\left| \left[\bigcap_{i=1}^{n-1} (P_i) \cap (P) \right] \backslash (Q) \right| \geq 1.$$

Hence $\mathcal{K}$ is a G_n-KDP. □

Theorem 1. *For $n \geq 2$, any $(n+1)$-(v, k, λ) design is a G_n-KDP.*

Proof. We use the mathematical induction on n. Clearly it is true for $n = 2$ as 3-(v, k, λ) design is always an original KDP in [7]. Suppose t-(v, k, λ) design is a G_{t-1}-KDP. Let $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a $(t+1)$-(v, k, λ) design. Then the internal structure $\mathcal{K}_P (P \in \mathcal{P})$ of $\mathcal{K}$ is a t-design(see [5]). By assumption $\mathcal{K}_P$ is again a G_{t-1}-KDP. Therefore $\mathcal{K}$ is a G_t-KDP by Lemma 4. Thus a $(n+1)$-(v, k, λ) design is a G_n-KDP for all $n \geq 2$. □

Theorem 2. *A G_{n+1}-KDP $(n \geq 2)$ is always a G_n-KDP.*

Proof. Suppose that $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is a G_{n+1}-KDP with $n \geq 2$. Then for any distinct n users $P_1, P_2, \cdots, P_n \in \mathcal{P}$ we can choose $v - n$ further users $Q_1, Q_2, \cdots Q_{v-n} \in \mathcal{P}$ distinct from $P_1, P_2, \cdots, P_n$. Every set of n+1 users in a G_{n+1}-KDP is uniquely incident with at least one common subkey, i.e., $| \bigcap_{i=1}^{n}(P_i) \cap (Q_j) | \geq 1$ for all j and $\bigcap_{i=1}^{n}(P_i) \cap (Q_j) \not\subseteq \bigcap_{i=1}^{n}(P_i) \cap (Q_k)$ for all $1 \leq j, k \leq v - n$ with $j \neq k$. Hence $\bigcap_{i=1}^{n}(P_i) \not\subseteq (Q_j)$ for all j. Therefore $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is also an G_n-KDP. □

According to the above theorem, we note that G_{n+1}-KDP $\subset G_n$-KDP $\subset G_{n-1}$-KDP $\subset \cdots$ $(n \geq 2)$. The following construction demonstrates how we have a maximal m such that $\mathcal{K}$ is a G_m-KDP but not a G_{m+1}-KDP.

Constructing the maximal m from a G_n-KDP $\mathcal{K}$

Firstly represent the G_n-KDP $\mathcal{K}$ as a $v \times b$ incidence matrix $A = (a_{ij})$ as previously shown.

Step 1. For column j,
if row i is 1, i.e., $a_{ij} = 1$, then add P_i to set x_j,
else skip.
Once this is complete for $j = 1, 2, \cdots, b$ and $i = 1, 2, \cdots, v$ we should have b subsets $x_1, x_2, \cdots, x_b$ of users.
Step 2. For $k \neq l$ $(k, l = 1, 2, \cdots b)$,

if $x_k \not\subseteq x_l$ *and* $x_l \not\subseteq x_k$*, let* $x_k \bigcap x_l = x_{(k)(l)}$ *and*
if $|x_{(k)(l)}| \geq 2$ *and* $x_{(k)(l)}$ *is the new one, then save* $x_{(k)(l)}$*,*
else skip.
Step 3. Repeat Step 2 for all subsets of users from Step 1 and Step 2. Continue until no new subsets of users are produced.
Step 4. Classify x_j *according to the number of users.*
Set $x^{(n)} = \{j : |x_j| = n\}$ $(1 \leq n \leq v)$.
Step 5. For $n = 1, 2, \cdots, v$,
check the cardinal number $|x^{(n)}| = \binom{v}{n}$ *or not.*
The number $m = max\{n : |x^{(n)}| = \binom{v}{n}\}$ *makes up the maximal* m *such that* $\mathcal{K}$ *is a* G_m*-KDP but not a* G_{m+1}*-KDP.*

Example 2. Consider the G_3-KDP in Examples 1 (3)

$$A = (a_{ij}) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Let's now find the maximal m from the given incidence matrix A.
Step 1. We get 8 subsets of users $x_1 = \{P_1, P_3, P_4, P_5\}$, $x_2 = \{P_1, P_2, P_4, P_5\}$, $x_3 = \{P_1, P_2, P_3, P_5\}$, $x_4 = \{P_1, P_3, P_4\}$, $x_5 = \{P_1, P_2, P_4\}$, $x_6 = \{P_1, P_2, P_3\}$, $x_7 = \{P_2, P_3, P_4, P_5\}$ and $x_8 = \{P_2, P_3, P_4\}$ from each subkey.
Step 2. We have 12 new subsets of users $x_{(1)(2)} = \{P_1, P_4, P_5\}$, $x_{(1)(3)} = \{P_1, P_3, P_5\}$, $x_{(1)(5)} = \{P_1, P_4\}$, $x_{(1)(6)} = \{P_1, P_3\}$, $x_{(1)(7)} = \{P_3, P_4, P_5\}$, $x_{(1)(8)} = \{P_3, P_4\}$, $x_{(2)(3)} = \{P_1, P_2, P_5\}$, $x_{(2)(6)} = \{P_1, P_2\}$, $x_{(2)(7)} = \{P_2, P_4, P_5\}$, $x_{(2)(8)} = \{P_2, P_4\}$, $x_{(3)(7)} = \{P_2, P_3, P_5\}$ and $x_{(3)(8)} = \{P_2, P_3\}$ by intersecting the subsets of users in Step 1.
Step 3. We also have 4 more subsets of users $x_{(3)(12)} = \{P_1, P_5\}$, $x_{(7)(12)} = \{P_4, P_5\}$, $x_{(7)(13)} = \{P_3, P_5\}$ and $x_{(7)(23)} = \{P_2, P_5\}$ by repeating Step 2 for all subsets of users from Step 1 and Step 2.
Step 4. We set $x^{(2)} = \{(1)(5), (1)(6), (1)(8), (2)(6), (2)(8), (3)(8), (3)(12), (7)(12), (7)(13), (7)(23)\}$, $x^{(3)} = \{4, 5, 6, 8, (1)(2), (1)(3), (1)(7), (2)(3), (2)(7), (3)(7)\}$ and $x^{(4)} = \{1, 2, 3, 7\}$.
Step 5. We check $|x^{(2)}| = 10 = \binom{5}{2}$, $|x^{(3)}| = 10 = \binom{5}{5}$ and $|x^{(4)}| = 4 \neq 5 = \binom{5}{2}$. Hence we take $m = max\{2, 3\} = 3$, i.e., the given incidence matrix A represents G_3-KDP and also G_2-KDP, but not a G_4-KDP.

A known difficulty with the original KDP has been suggested by Blom[2] is the problem of collusion. He pointed out the shortcomings of such a system if two or more users collude and pool their sets of subkeys then the system can easily be broken. To consider the problem of collusion in G_n-KDP, we would require a system which was secure against collusion by up to some number $w \geq 1$ of users.

This genenral concept was introduced by Mitchell and Piper[6] as a further developments. They called it *a (n, w)-collusion resistant KDP* and defined by for any n-subset $F = \{f(1), f(2), \cdots, f(n)\}$ and w-subset $H = \{h(1), h(2), \cdots, h(w)\}$ of $\{1, 2, \cdots, v\}$ respectively, $\bigcap_{i=1}^{n}(P_{f(i)}) \subset \bigcup_{j=1}^{w}(P_{h(j)})$ if and only if $F \cap H \neq \emptyset$.

We denote this by G_n^w-KDP since it is a w-collusion resistent G_n-KDP. This property ensures that the key shared by any n-pair of users can not be compromised by any colluding set of w or fewer other users since no other set of w other users hold all the subkeys which the n-pair of users have in common.

We now provide some equivalent properties of G_n^w-KDP for $w \geq 1$.

Lemma 3. *Let $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a finite incidence structure. Then the following concepts are equivalent:*

(1) $\mathcal{K}$ is a G_n^w-KDP.

For any n users $P_1, P_2, \cdots, P_n \in \mathcal{P}$ and any w users $Q_1, Q_2, \cdots, Q_w \in \mathcal{P}$ distinct from P_i $(1 \leq i \leq n)$,

(2) $| \bigcap_{i=1}^{n}(P_i) \setminus \bigcup_{j=1}^{w}(Q_j) | \geq 1$.

(3) $\{x_j : \{P_1, P_2, \cdots, P_n\} \subset x_j$ and $\bigcup_{i=1}^{w}(Q_i) \cap x_j = \emptyset\}$ is nonempty.

Proof. For a G_n^w-KDP $\mathcal{K}$, suppose $| \bigcap_{i=1}^{n}(P_i) \setminus \bigcup_{i=1}^{w}(Q_i) | < 1$ for some users $P_1, P_2, \cdots, P_n$ and $Q_1, Q_2, \cdots, Q_w$, that is, $\bigcap_{i=1}^{n}(P_i) \setminus \bigcup_{i=1}^{w}(Q_i) = \emptyset$. Hence $\bigcap_{i=1}^{n}(P_i) \subset \bigcup_{i=1}^{w}(Q_i)$. By assumption, $P_i = Q_j$ for some i and j. This is a contradiction since all users are distinct.

Since (2) means that there exists a subkey in $\mathcal{K}$ which is incident with $P_1, P_2, \cdots, P_n$ but which is not incident with $Q_1, Q_2, \cdots, Q_w$, then it follows (2) is equivalent to (3).

To show (3) implies (1), suppose that there are $n + w$ users P_i and Q_j $(1 \leq i \leq n, 1 \leq j \leq w)$ such that $\bigcap_{i=1}^{n}(P_i) \subset \bigcup_{j=1}^{w}(Q_j)$, which contradicts the assumption (3). This completes the proof. □

Example 3. (1) A trivial G_n-KDP is clearly a G_n^w-KDP for every w.

(2) Any $(n + w)$-design is a G_n^w-KDP $(n, w \geq 1)$(see [6]).

Now we have the following facts immediately.

(1) Any G_n-KDP is a G_n^w-KDP for some $w \geq 1$.

(2) If $\mathcal{K}$ is a G_n^w-KDP, then $\mathcal{K}$ is also a $G_n^{w'}$-KDP for all w' $(1 \leq w' \leq w)$.

3. Generalization of Quinn's bounds for the number of subkeys

In 1999, K. Quinn[9] had made two lower bounds for the number of subkey at each user P. These were for w-collusion resistent KDP, i.e., G_2^w-KDP. We denote the number of subkeys incident with a user P by r_P as usual.

The first one is that for any user P in $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, $r_P \geq w\{log_2(v - 1) - log_2 w\}$[7,9]. We have a generalization of this bound for a G_n^w-KDP with v users as follows.

Theorem 3. *For a G_n^w-KDP $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ with v users and a user $P \in \mathcal{P}$,*

$$r_P \geq w\left[log_2\binom{v-1}{n-1} - log_2 w\right].$$

Moreover, the lower bound for the total number of subkeys in $\mathcal{K}$ is

$$\binom{v}{n} w\{log_2(v-1)\cdots(v-n+1) - \log_2(n-1)! - \log_2 w\}.$$

Proof. For any user $P \in \mathcal{P}$, consider the $\binom{v-1}{n-1}$ elements set

$$\left\{(P) \cap \bigcap_{i=1}^{n-1}(Q_i) \mid Q_i \in \mathcal{P}\backslash\{P\}, 1 \leq i \leq n-1\right\}.$$

We claim that the $\binom{\binom{v-1}{n-1}}{w}$ possible unions of w elements of this set form a Sperner System with ground set (P). Because suppose for $P \in \mathcal{P}$, we have

$$\left[(P)\cap\bigcap_{i=1}^{n-1}(Q_{1i})\right]\bigcup\cdots\bigcup\left[(P)\cap\bigcap_{i=1}^{n-1}(Q_{wi})\right]$$

$$\subset \left[(P)\cap\bigcap_{j=1}^{n-1}(R_{1j})\right]\bigcup\cdots\bigcup\left[(P)\cap\bigcap_{j=1}^{n-1}(R_{wj})\right],$$

where there is a set $\{Q_{k1}, \cdots, Q_{k(n-1)}\}$ of users on the left which is not one of the sets $\{R_{11}, \cdots, R_{1(n-1)}\}, \cdots, \{R_{w1}, \cdots, R_{w(n-1)}\}$ on the right. Then for this set of users,

$$(P)\cap\bigcap_{i=1}^{n-1}(Q_{ki}) \subset \left[\bigcap_{j=1}^{n-1}(R_{1j})\right]\cup\cdots\cup\left[\bigcap_{j=1}^{n-1}(R_{wj})\right] = \bigcup_{k=1}^{w}\left[\bigcap_{j=1}^{n-1}(R_{kj})\right]$$

which contradicts the assumption that $\mathcal{K}$ is a G_n^w-KDP. Applying Sperner's theorem[1,6] and the known fact gives

$$2^{r_P-1} \geq \binom{r_P}{[\frac{r_P}{2}]} \geq \binom{\binom{v-1}{n-1}}{w} \Longrightarrow 2^{r_P-1} \geq \left\{\frac{\binom{v-1}{n-1}}{w}\right\}^w.$$

So $r_P - 1 \geq w\{log_2\binom{v-1}{n-1} - log_2 w\} = w\{log_2(v-1)\cdots(v-n+1) - \log_2(n-1)! - \log_2 w\}$. For the second statement, we note that the total number of n-pairs in $\mathcal{K}$ is $\binom{v}{n}$. Thus, the result follows. □

Remark. It should be clear from the above theorem that for a G_n-KDP with v users and any user P, $r_P \geq log_2\binom{v-1}{n-1}$, since this case is for $w = 1$.

The second one is the following: for any user $P \in \mathcal{P}$, $r_P \geq min\{v-1, \frac{1}{2}(w+1)(w+2)\}$[9]. We have a generalization of this bound for a G_n^w-KDP with v users as follows. We begin by explaining a generalization of Lemma in [9].

Lemma 4. *Let $P_1, P_2, \cdots, P_n$ be any n users of G_n^w-KDP such that each subkey in $\bigcap_{i=1}^n (P_i)$ is held by at least one other user. Then for any $\mathcal{S} \subset \mathcal{P} \backslash \{P_1, P_2, \cdots, P_n\}$ with $0 \leq |\mathcal{S}| \leq w$,*

$$\left| \bigcap_{i=1}^{n} (P_i) \backslash \bigcup_{Q \in \mathcal{S}} (Q) \right| \geq w + n - 1 - |\mathcal{S}| .$$

Proof. We have the result by applying the equivalent definition of G_n^w-KDP and the similar ways in Quinn's proof[9]. Suppose not, that is, let $\mathcal{S}$ be a maximal subset of $\mathcal{P} \backslash \{P_1, P_2, \cdots, P_n\}$ with $0 \leq \mathcal{S} \leq w$ such that $| \bigcap_{i=1}^n (P_i) \backslash \bigcup_{Q \in \mathcal{S}} (Q) | \leq w + n - 2 - |\mathcal{S}|$. Since $\mathcal{K}$ is a G_n^w-KDP,

$$\left| \bigcap_{i=1}^{n} (P_i) \backslash \bigcup_{Q \in \mathcal{S}} (Q) \right| \geq 1$$

and hence from two above inequalities, we have $|\mathcal{S}| \leq w + n - 3$. By the second inequality and the assumption, some user $Q' \in \mathcal{P} - [\mathcal{S} \bigcup \{P_1, P_2, \cdots, P_n\}]$ must hold a subkey in $\bigcap_{i=1}^n (P_i)$. Therefore

$$\left| \bigcap_{i=1}^{n} (P_i) \backslash \bigcup_{Q \in \mathcal{S} \bigcup \{Q'\}} (Q) \right| \leq (w + n - 2 - |\mathcal{S}|) - 1 = w + n - 3 - |\mathcal{S}| .$$

This is a contradiction that $\mathcal{S}$ is maximal. This completes the proof. □

In particular, if $w = 1$, $| \bigcap_{i=1}^n (P_i) \backslash \bigcup_{Q \in \mathcal{S}} (Q) | \geq n - |\mathcal{S}|$(see [9]).

Theorem 4. *For any G_n^w-KDP $\mathcal{K}$ with v users and any user P with $r_P < v - (n-1)$,*

$$r_P \geq \frac{1}{2}(w + n - 1)(w + n).$$

Moreover, the lower bound for the total number of subkeys in $\mathcal{K}$ is

$$\frac{1}{2}\binom{v}{n}(w + n - 1)(w + n).$$

Proof. For any $P \in \mathcal{P}$, let $\mathcal{S}$ be the set of all users in $\mathcal{P} - \{P\}$ such that every subkey held by any $n-1$ users and by P is also held by a third user. Let $\mathcal{S}'$ consist of all other users in $\mathcal{P} - \{P\}$, those which hold a subkey held by P which is held by no third user. Then $|\mathcal{S}'| = v - 1 - |\mathcal{S}|$. We claim that $|\mathcal{S}| \geq w + n$. Since P has a different subkey in common with every user in $\mathcal{S}'$, $r_P \geq v - 1 - |\mathcal{S}|$. Also we note that $r_P < v - (n-1)$ from the assumption and hence $|\mathcal{S}| \geq n - 1$. Let $P_1, P_2, \cdots, P_{n-1} \in \mathcal{S}$. By the above lemma, $| \bigcap_{i=1}^{n-1} (P_i) \cap (P) | \geq w + n - 1$. Also P has at least one distinct subkey not held by $P_1, P_2, \cdots, P_{n-1}$ in common with every user in $\mathcal{S}'$. Hence

$$r_P \geq (w + n - 1) + (v - 1 - |\mathcal{S}|) = w + n + v - 2 - |\mathcal{S}|$$

Thus $v-1 > w+n+v-2- \mid \mathcal{S} \mid$. Therefore we have our claim $\mid \mathcal{S} \mid \geq w+n$. Let $\{Q_1, Q_2, \cdots, Q_{w+n-1}\} \subset \mathcal{S}$. Then by Lemma 4, for $0 \leq j \leq w+n-2$,

$$\left| \left[(P) \cap \bigcap_{k=j+1}^{j+n-1} (Q_{ik}) \right] \setminus \bigcup_{k=1}^{j} (Q_{ik}) \right| \geq w+n-1-j.$$

So

$$\begin{aligned} r_P &\geq (w+n-1)+(w+n-2)+\cdots+1 \\ &= \tfrac{1}{2}(w+n-1)(w+n) \end{aligned}$$

as stated.

For the second statement, we note again that the total number of n-pairs in $\mathcal{K}$ is $\binom{v}{n}$. □

References

1. S. R. Blackburn and F. Piper, *Applications of combinatorics to security*, Proceedings of The Applications of Combinatorial Mathematics, Oxford, 14-16 December 1994, C. Mitchell (Ed.) (Oxford University Press, Oxford, 1997), 31-47.
2. R. Blom, *Non-public key distribution*, Advances in Cryptology: Proceedings of Crypto 82, Plenum Press, New York(1983), 231-236.
3. M. Dyer, T. Fenner, A. Frieze and A. Thomason, *On key storage in secure networks*, J. Cryptology, **8** (1995), 189-200.
4. L. Gong and D. L. Wheeler, *A matrix key distribution scheme*, J. Cryptology, **2** (1990), 51-59.
5. D. Hughes and F. Piper, *Design Theory*, Cambridge University Press, Cambridge, 1985.
6. C. Mitchell and F. C. Piper, *Key storage in secure networks*, Discrete Applied Mathematics, **21** (1988) 215-228.
7. K. A. S. Quinn, *Combinatorial structures with applications to information theory*, Doctoral Thesis, University of London, 1991.
8. K. A. S. Quinn, *Some constructions for key distribution patterns*, Designs, Codes and Cryptography, **4** (1994), 177-191.
9. K. A. S. Quinn, *Bounds for key distribution patterns*, J. Cryptology, **12:4** (1999), 227-240.
10. D. R. Stinson and T. V. Trung, *Some new results on key distribution patterns and broadcast encryption*, Designs, Codes and Cryptography, **14** (1998), 261-279.

Seon Ho Shin is a full-time lecturer in Mathematics at Soongsil University. She received her Ph.D at Sookmyung Womens University. Her research interests include key distributions, and mathematical aspects of cryptography.

Department of Mathematics, Soongsil University, Seoul 156-743, Korea
e-mail: `shinsh@ssu.ac.kr`

Julia C. Bate is a PhD student in Mathematics at Royal Holloway, University of London. She is researching methods of key management using combinatorial techniques.

Department of Mathematics, Royal Holloway, University of London, Egham, Surrey TW20 0EX, U.K.
e-mail: `J.C.Bate@rhul.ac.uk`