Light-Weight Key Predistribution Scheme with Key Renewal

Alexey V. Urivskiy

ourivski@mail.ru

JSC Infotecs, Moscow

Set-intersection key predistribution schemes

- a network of N nodes
- a set of secret keys $\mathcal{K}$ — the key pool of V keys
- a set of node's keys $\mathcal{S}_j \subset \mathcal{K}$ — the node's key block of r keys
- a pairwise key $\kappa_{j_1 j_2} = KDF(\mathcal{S}_{j_1} \bigcap \mathcal{S}_{j_2})$

Definition: A set-intersection key predistribution scheme is w-secure if for $\forall$ j_1, j_2 and $\{k_1, \ldots, k_w\}$: $\{j_1, j_2\} \bigcap \{k_1, \ldots, k_w\} = \emptyset$ it holds

$$\mathcal{S}_{j_1} \bigcap \mathcal{S}_{j_2} \not\subseteq \bigcup_{i=1}^{w} \mathcal{S}_{k_i}.$$

- w-secure SIS is equivalent to $(2, w)$ cover-free family

Incidence Matrix

An incidence matrix of a SIS is a binary $V \times N$ matrix $\mathbf{A} = [a_{ij}]$:
$a_{ij} = 1$ if $\kappa_i \in \mathcal{S}_j$,
$a_{ij} = 0$ otherwise.

Example: An incidence matrix of 2-secure SIS for 4 nodes:

$$\mathbf{A} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} .$$

Problem

For a given N and w

construct w-secure SIS

with a smallest size r of node's key block.

Half-Weight Columns

Definition: A binary half-weight column $\mathbf{b}$ is an m-column: $w_H(\mathbf{b}) = \frac{m}{2}$.

Collect half-weight columns into matrix $\mathbf{B}$:

- at most $\frac{1}{2}\binom{m}{m/2}$ half-weight columns of length m
- all columns are different
- no complementary columns in $\mathbf{B}$

$\overline{\mathbf{B}}$ is complementary to $\mathbf{B}$.

Example:

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \quad \overline{\mathbf{B}} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

1-secure Scheme — Double-Complement Construction

Theorem: Let a $V_0 \times n_0$ incidence matrix $\mathbf{A}$ define at least a 1-secure SIS for n_0 nodes. Then

$$\mathbf{C} = \begin{bmatrix} \mathbf{A} & \mathbf{A} \\ \mathbf{B} & \overline{\mathbf{B}} \end{bmatrix}$$

is an incidence matrix of a 1-secure SIS for $2n_0$ nodes.

Here $\mathbf{B}$ and $\overline{\mathbf{B}}$ are $m \times n_0$ complementary matrices of half-weight columns of even length m, such that $\binom{m}{m/2} \geq 2n_0$.

Example

$$\mathbf{C} = \left[\begin{array}{cccc|cccc}
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
\hline
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0
\end{array}\right]$$

Practical Properties

Storage: Node's block size

$$r(N) = r_0 + \frac{\lg^2 N}{4} + O(\lg N \lg \lg N)$$

Key computation: a column of $\mathbf{C}$ can be computed in $O(\lg^2 N)$ operations on $O(\lg N)$-bit numbers $\Rightarrow$ non-interactive key computation

$$\mathbf{C} = \left[\begin{array}{c|c|c|c|cccc|c|c|c|c}
\mathbf{A} & \mathbf{A} & \mathbf{A} & \mathbf{A} & \cdots & \cdots & \cdots & \cdots & \mathbf{A} & \mathbf{A} & \mathbf{A} & \mathbf{A} \\ \hline
\mathbf{B}_2 & \overline{\mathbf{B}}_2 & \mathbf{B}_2 & \overline{\mathbf{B}}_2 & \cdots & \cdots & \cdots & \cdots & \mathbf{B}_2 & \overline{\mathbf{B}}_2 & \mathbf{B}_2 & \overline{\mathbf{B}}_2 \\ \hline
\multicolumn{2}{c|}{\mathbf{B}_3} & \multicolumn{2}{c|}{\overline{\mathbf{B}}_3} & \cdots & \cdots & \cdots & \cdots & \multicolumn{2}{|c|}{\mathbf{B}_3} & \multicolumn{2}{c}{\overline{\mathbf{B}}_3} \\ \hline
\multicolumn{4}{c|}{\mathbf{B}_4} & \cdots & \cdots & \cdots & \cdots & \multicolumn{4}{|c}{\overline{\mathbf{B}}_4} \\ \hline
\multicolumn{12}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots} \\ \hline
\multicolumn{6}{c|}{\mathbf{B}_I} & \multicolumn{6}{c}{\overline{\mathbf{B}}_I}
\end{array} \right] .$$

On Double-Complement Construction

Is Double-Complement construction useful
for producing w-secure schemes?

- $w = 1$ — this presentation
- $w = 2$ — construction due to Kim H. K. & Lebedev V.
- $w \geq 3$ — open question

Security

What to do when w is not large enough?

- Larger w: a known lower bound

$$r(N) \geq \max\left\{ w\left(\log_2(N-1) - \log_2 w\right), \min\left\{\frac{1}{2}(w+1)(w+2), N-1\right\}\right\}$$

For $w \gtrsim \sqrt{2N}$ only the trivial scheme useful with $r(N) = N-1$.

- Probabilistic key predistribution: $\exists j_1$ and j_2 s.t. $\mathcal{S}_{j_1} \bigcap \mathcal{S}_{j_2} = \emptyset$.
  - shared key discovery protocol to find $\mathcal{S}_{j_1} \bigcap \mathcal{S}_{j_2}$ if any
  - a path-key establishment protocol
    to find a sequence of nodes between j_1 and j_2
    so that every two adjacent nodes has a common key

- Key renewal

Key Renewal

If some c nodes $k_1, \ldots, k_c$ are compromised and for every $j \notin \{k_1, \ldots, k_c\}$

$$\mathcal{S}_j \not\subseteq \bigcup_{i=1}^{c} \mathcal{S}_{k_i},$$

then a key update K^* can be sent to every innocent node via a key from

$$\mathcal{S}(j, k_1, \ldots, k_c) = \mathcal{S}_j \setminus \bigcup_{i=1}^{c} \mathcal{S}_{k_i}$$

Key renewal process:

- broadcast $E_\ell = E_{\kappa_\ell}(K^*)$ for every j and $\kappa_\ell \in \mathcal{S}(j, k_1, \ldots, k_c)$
- renew all keys: $\kappa^* = KDF(\kappa, K^*)$ on every node

Definition: The key renewal threshold is the largest s for which $\mathcal{S}_j \not\subseteq \bigcup_{i=1}^{s} \mathcal{S}_{k_i}$ for any $\{k_1, \ldots, k_s\}$ and any $j \notin \{k_1, \ldots, k_s\}$.

Combinatorial Problem

For a given N, w and s construct a $(2, w)$-cover-free family which is also a $(1, s)$-cover free family.

What is the relation between N, w, s and r?

Coverings

Definition: A covering $\mathcal{S}_c$ with respect to $\{k_1, \ldots, k_c\}$ is a set such that $\mathcal{S}_c \bigcap \mathcal{S}(j, k_1, \ldots, k_c) \neq \emptyset$ for every $j \notin \{k_1, \ldots, k_c\}$

Results:

- The key renewal threshold is 2 —
  given construction defines $(2, 1)$ and $(1, 2)$ cover-free family
- The cardinality of a minimal covering $\chi \leq \chi_{\mathbf{A}} + \log \dfrac{N}{n_0}$
- The complexity of finding a covering is $O(\lg N)$ bitwise operations on $O(\lg N)$-bit vectors

Thank you!

Questions?