Secure Shuffling

And its impact on d-Privacy

MACQUARIE University
SYDNEY·AUSTRALIA

Svyatoslav Kushnarev & Vladimir Balygin

Faculty of Science and Engineering

School of Computing, Macquarie University

Context

In the modern internet era, businesses and governments regularly monitor customers' personal data, leading to targeted advertising and increased privacy risks. To combat this, privacy laws like EUGDPR are adopted.

They, however, require technical implementation via algorithms, hence ***d-Privacy***, a mechanism using randomisation and probabilistic methods, was created to protect against breaches and misuse.

It masks sensitive information by adding controlled random noise to data, and has been enhanced with secure shuffling mechanisms.

Challenge

Since ***Secure Shuffling*** is utilized in various critical systems such as ***voting systems*** and ***online auctions***, it is necessary to consistently study this algorithm and evaluate its effectiveness as a security tool in a regular manner. To this end, we will consider three variants of the algorithm: complete shuffling, preserve-partition shuffling, and Kronecker product.

Complete shuffling

Algorithm 1 Complete shuffling

input channel
select randomly a permutation σ of $(x_1, x_2, x_3, ...)$
$x = \sigma(s)$
apply the channel
output channel

Theorem:

After the ***complete shuffling*** the ***zero leakage*** channel will ***always*** be obtained.

The ***multiplicative capacity*** is the ***maximum multiplicative Bayes leakage*** over all priors.

Example:

Input channel

C	y_0	y_1	y_2
x_0	1/2	1/4	1/4
x_1	1/4	1/2	1/4
x_2	1/4	1/4	1/2

$\longrightarrow$

Output channel

C	y_0	y_1	y_2
x_0	1/3	1/3	1/3
x_1	1/3	1/3	1/3
x_2	1/3	1/3	1/3

Capacity Before

$$cap = \frac{3}{2}$$

Capacity After

$$cap = 1$$

References

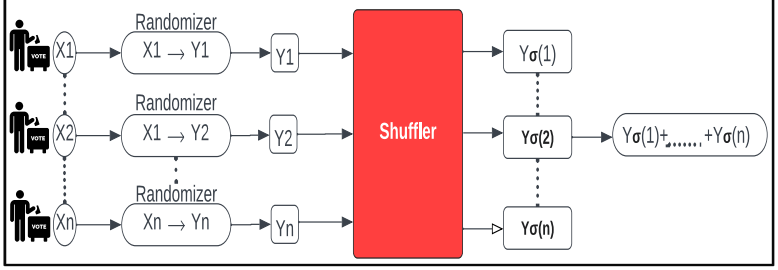
1. Alvim, MS, Chatzikokolakis, K, McIver, A, Morgan, C, Palamidessi, C & Smith, G 2020, The Science of Quantitative Information Flow. Information Security and Cryptography, Springer, Springer Nature, Cham, Switzerland. https://doi.org/10.1007/978-3-319-96131-6.
2. Peng, K. (2011) 'An efficient shuffling based evoting scheme', Journal of Systems and Software, 84(6), pp. 906–922. doi:10.1016/j.jss.2011.01.001.

Secure shuffling

Secure shuffling is a method used in ***electoral voting*** to ensure correctness, privacy, and verifiability.

Votes are ***encrypted*** using special receipts that confirm the vote and hide its contents. These receipts are then ***shuffled*** by a ***trusted service*** called a "mixnet," where an algorithm reassembles input ciphertexts into a ***permutation*** at the output. The algorithm must be kept secret to de-encrypt the output ciphertexts and recover the original input ciphertexts.

Shuffling scheme



Preserve-partition shuffling

Algorithm 2 Shuffling with preserving the partition

1. input channel
2. select randomly a permutation that preserves the partitions
3. apply permutation
4. apply the channel
5. output channel

Theorem:

The capacity of the ***preserve-partition shuffled channel*** is ***less than*** the capacity of the original channel.

Example:

Input channel

C	y_0	y_1	y_2
x_0	1/2	1/4	1/4
x_1	1/4	1/2	1/4
x_2	1/4	1/4	1/2

$\longrightarrow$

Output channel

C	y_0	y_1	y_2
x_0	3/8	3/8	1/4
x_1	3/8	3/8	1/4
x_2	1/4	1/4	1/2

Capacity Before

$$cap = \frac{3}{2}$$

Capacity After

$$cap = \frac{5}{4} \longrightarrow cap_{before} > cap_{after}$$

Kronecker product

Theorem:

$$Cap(\mathbb{A} \otimes \mathbb{B}) = Cap(\mathbb{A}) \times Cap(\mathbb{B}) \quad \text{and} \quad Cap(\mathbb{A} \otimes \mathbb{B}) = Cap(\mathbb{B} \otimes \mathbb{A})$$

Example: Assume we are given the following channels:

$$\mathbb{A} = \begin{pmatrix} 1/3 & 2/3 \\ 2/3 & 1/3 \end{pmatrix}, \quad \mathbb{B} = \begin{pmatrix} 3/5 & 2/5 \\ 2/5 & 3/5 \end{pmatrix}$$

$$\mathbb{A} \otimes \mathbb{B} = \begin{pmatrix} 1/5 & 2/5 & 2/15 & 4/15 \\ 2/5 & 1/5 & 4/15 & 2/15 \\ 2/15 & 4/15 & 1/5 & 2/5 \\ 4/15 & 2/15 & 2/5 & 1/5 \end{pmatrix} \quad \mathbb{B} \otimes \mathbb{A} = \begin{pmatrix} 1/5 & 2/5 & 2/15 & 4/15 \\ 2/5 & 1/5 & 4/15 & 2/15 \\ 2/15 & 4/15 & 1/5 & 2/5 \\ 4/15 & 2/15 & 2/5 & 1/5 \end{pmatrix}$$

$$cap(\mathbb{A} \otimes \mathbb{B}) = \frac{8}{5} \qquad cap(\mathbb{B} \otimes \mathbb{A}) = \frac{8}{5}$$

svyatoslav.kushnarev@students.mq.edu.au
vladimir.balygin1@students.mq.edu.au

Designer : Roman Leonov