SEKRET

System Ewaluacji Kryptograficznej Rejestru Ewidencji Tajnych

Opiekun: prof. UAM dr hab. Maciej Grześkowiak *Jakub Grzelak*

Opis projektu

Celem projektu SEKRET jest stworzenie platformy do wykonywania zapytań na zbiorach danych niejawnych - takich, do których użytkownik nie może mieć bezpośredniego wglądu, a których bezpieczeństwo zapewnione jest dzięki mechanizmom kryptograficznym i matematyce. Umożliwione zostanie wykonywanie różnych rodzajów zapytań, w zależności od potrzeb użytkownika. Aplikacja zapewnia pełną tajność treści zapytań.

Protokół PSI-CA

W projekcie użyty został protokół **PSI-CA** (**Private Set Intersection Cardinality**), w którym dwie strony komunikacji (klient, serwer) posiadając swoje **tajne** zbiory danych chcą ustalić moc części wspólnej swoich zbiorów. Zbiór klienta stanowi treść zapytania, a zbiorem serwera jest cały zbiór danych przechowywany na serwerze.

Protokół zapewnia:

- **Prywatność serwera** - klient nie dowiaduje się nic, poza wielkością zbioru serwera oraz mocą części wspólnej zbiorów
- **Prywatność klienta** - serwer nie dowiaduje się nic, poza wielkością zbioru klienta
- **Nielinkowalność** - żadna ze stron nie może ustalić, czy jakiekolwiek dwie instancje protokołu są ze sobą powiązane, tzn. czy zostały wykonane na tych samych danych wejściowych.

Protokół PSI / PSI-CA znajduje współcześnie wiele zastosowań, np. wykrywanie botów, ataków DoS, udostępnianie lokalizacji lub w grach.

Wykonywanie zapytania

Klient

$$H : \{0,1\}^* \to Z_p^* \quad H' : \{0,1\}^* \to \{0,1\}^\kappa$$
$$R_c \leftarrow Z_q$$
$$C = \{c_1, \ldots, c_n\}$$

Imię	Nazwisko	Uczelnia	Wiek
Jan	Kowalski	UAM	25

$$\forall_i 1 \le i \le n$$
$$hc_i = H(c_i) \,\%\, p$$
$$a_i = hc_i^{R_c} \,\%\, p$$

9403 1406	08065038 50384394	180717148 437542087	1340 3129

$$\forall_i 1 \le i \le n$$
$$bc_i = (a'_i)^{1/R_c \,\%\, q} \,\%\, p$$

9403 1403	08045038 50383494	180717148 4378650	4350 6123

$$\forall_i 1 \le i \le n$$
$$tc_i = H'(bc_i)$$

94ad 140d	a80f5038 5038cd9d	b80717b48 ec7fec0	1340 3129

$$|\{ts_1, \ldots, ts_m\} \cap \{tc_1, \ldots, tc_n\}|$$

94ad 140d	a80f5038 5038cd9d	b80717b4 8ec7fec0	bd40 31b9
944d 140d	87449e7d 385d2652	03de17df b94ddc0e	0007 3da3
5aba 68ab	5a06844f 96483bee	779e504d 3fde90eb	04d3 fde9

Serwer

$$S = \{s_1, \ldots, s_m\} \; R_s \leftarrow Z_q$$
$$(\hat{s_1}, \ldots, \hat{s_m}) \leftarrow \Pi(S)$$
$$\forall_i 1 \le i \le m$$
$$hs_i = H(\hat{s_i}) \,\%\, p$$
$$bs_i = hs_i^{R_s} \,\%\, p$$
$$ts_i = H'(bs_i)$$

94ad 140d	a80f5038 5038cd9d	b80717b4 8ec7fec0	bd40 31b9
944d 140d	87449e7d 385d2652	03de17df b94ddc0e	0007 3da3
5aba 68ab	5a06844f 96483bee	779e504d 3fde90eb	04d3 fde9

9403 1403	08065038 50383495	180717148 767893158	1340 3129

$$(\hat{a_1}, \ldots, \hat{a_n}) \leftarrow \Pi'(a_1, \ldots, a_n)$$
$$\forall i \; 1 \le i \le n : a'_i = \hat{a_i}^{R_s} \,\%\, p$$

Schemat przedstawia przykład przetwarzania danych w ramach protokołu PSI-CA na potrzeby zapytania I rodzaju.

W wyniku przeprowadzenia protokołu, jeśli dany element użytkownika faktycznie należy do zbioru danych, użytkownik uzyska poprawny rezultat potwierdzający tę przynależność.

Rodzaje zapytań

I Należenie elementu do zbioru

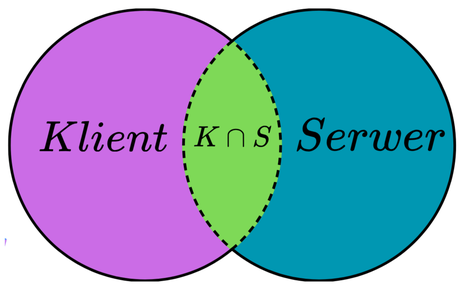
Użytkownik może sprawdzić, czy dany element należy do zbioru danych, np. czy jego hasło znajduje się w bazie skompromitowanych haseł.

II Statystyki

Użytkownik może wygenerować statystyki ilościowe dotyczące wybranych parametrów, np. ile pracowników pracuje w poszczególnych działach.

III Część wspólna zbiorów

Użytkownik może sprawdzić, nie tylko ile, ale jakie elementy jego zbioru należą do zbioru danych serwera.



Źródła

"Fast and Private Computation of Cardinality of Set Intersection and Union" https://eprint.iacr.org/2011/141.pdf