A jednak się da (IX),

czyli saga kryptologiczna w odcinkach. Tym razem: o obliczeniach wielopodmiotowych.

Tomasz KAZANA

Niniejszy odcinek jest ostatni z serii. Przez niemal rok, wraz z Łukaszem Rajkowskim, próbowaliśmy pokazać Czytelnikowi, co ciekawego, a przede wszystkim – co zaskakującego, wiąże się z kryptologią. Naszą wielką nagrodą będzie, gdy – po przeczytaniu tych 9 odcinków – choć niewielka część Czytelników chociaż przez chwilę zawaha się, gdy w życiu codziennym będzie stwierdzać, że **czegoś się nie da...**

Punktem wyjścia naszych rozważań będzie podział sekretu pomiędzy n osób (o którym pisaliśmy więcej w Δ^2_{11}). To znaczy: załóżmy, że chcemy pewną tajną liczbę

$$x \in \{0, 1, \ldots, p-1\}$$

(p to pewna ustalona duża liczba pierwsza, np. $p = 191347024000932780814494239 17$) *rozproszyć* pomiędzy zbiór osób $A = (A_1, \ldots, A_n)$ w taki sposób, aby:

- każda z nich dostała pewien udział w postaci liczby $x_i \in \{0, \ldots, p-1\}$, oraz
- dowolna ich t-osobowa podgrupa nie była w stanie odtworzyć x (analizując swoje udziały), ale już (każda) podgrupa $(t+1)$-osobowa zawsze mogła to zrobić.

Powyższy problem da się rozwiązać dla dowolnego $0 \leqslant t \leqslant (n-1)$, szczegóły znajdują się w artykule cytowanym wyżej. Ogólna idea (pochodząca od Adiego Shamira) polega na tym, że losujemy dowolny wielomian w stopnia t (o współczynnikach $w_i \in \{0, \ldots, p-1\}$) o wyrazie wolnym równym x. Następnie ustalamy dowolne niezerowe (i parami różne) elementy y_i i określamy

$$x_i := (w(y_i) \bmod p).$$

Okazuje się, że tak zdefiniowane udziały spełniają nasze pierwotne założenia. Dziś jednak będziemy chcieli osiągnąć znacznie więcej. To znaczy, zapragniemy na podzielonych sekretach rachować!

Przyjmijmy, że sekrety są dwa: $a, b \in \{0, \ldots, p-1\}$ oraz że osoba o numerze i ma udziały w obu (w postaci liczb $a_i, b_i \in \{0, \ldots, p-1\}$). Chcemy teraz opracować taki *protokół*, który umożliwi wszystkim n osobom dokonanie wspólnych obliczeń, po których osoba i otrzyma pewną wartość c_i. Oczekujemy, że tak obliczone elementy $\{c_i\}_{1 \leqslant i \leqslant n}$ razem będą stanowić podział sekretu dla (rozważamy trzy przypadki):

1. $c = a + b \pmod p$;
2. $c = k \cdot a \pmod p$ (k jest publicznie znaną stałą);
3. $c = a \cdot b \pmod p$.

Prezentowane w tym artykule protokoły są bezpieczne w modelu pasywnym, tzn. zakładamy, że uczestnicy nie oszukują (nie wysyłają niepoprawnych komunikatów), a są tylko ciekawscy i chcieliby – z tego co legalnie widzą – wywnioskować więcej, niż być może powinni (mogą również działać w porozumieniu). Dodatkowo musimy założyć $t < n/2$ oraz przyjąć, że co najwyżej t uczestników jest w zmowie. W przypadku przeciwników aktywnych (oszukujących podczas protokołu) istnieją inne – bardziej skomplikowane – protokoły, które potrafią zapewnić bezpieczeństwo, gdy oszustów jest mniej niż $n/3$.

Banalne rozwiązanie polega na odtworzeniu a i b, obliczeniu c oraz dokonaniu nowego podziału, według oryginalnego protokołu. Nasz cel jest jednak ambitniejszy: chcemy rozproszyć c, ale w taki sposób, aby bezpośrednia informacja o a i b nie została na żadnym etapie przez nikogo (przez żadnego uczestnika bądź ich podgrupy o ograniczonej liczebności) jawnie odtworzona. Jak to zrobić?

Przypadek pierwszy i drugi jest łatwy (Zajmiemy się tylko pierwszym. Niech drugi pozostanie jako łatwe ćwiczenie.) i nie wymaga nawet żadnej komunikacji pomiędzy stronami. Wystarczy, że osoba i przyjmie $c_i := a_i + b_i \bmod p$ i wszystko będzie w porządku. Dlaczego? Przypomnijmy sobie tylko, czym jest a_i oraz b_i. Wiemy przecież, że

$$a_i = w_a(y_i) \pmod p \quad \text{oraz} \quad b_i = w_b(y_i) \pmod p,$$

dla pewnych wielomianów w_a oraz w_b. Wtedy oczywiście

$$a_i + b_i = (w_a + w_b)(y_i) \pmod p,$$

co oznacza, że (z definicji) elementy $a_i + b_i$ stanowią podział sekretu dla wyrazu wolnego wielomianu $(w_a + w_b)$ modulo p. Ten jednak wynosi $(a + b)$ modulo p, gdyż wyrazem wolnym w_a musi być a, a wyrazem wolnym w_b jest b.

Powyższe rozwiązanie rodzi pokusę, aby analogicznie rozwiązać przypadek trzeci. To znaczy, aby każda z osób przyjęła $c_i = a_i \cdot b_i \bmod p$, jako że $a \cdot b \pmod p$ jest wyrazem wolnym wielomianu $w_a \cdot w_b$ modulo p. Niestety, jest to rozwiązanie błędne. Problem bierze się stąd, że mnożenie dwóch wielomianów stopnia t

daje wielomian stopnia $2t$. A my przecież chcemy koniecznie otrzymać stopień t (w przypadku dodawania ten problem nie występował)! Rozwiązanie jest tutaj nieco bardziej skomplikowane.

Mnożenie podzielonych sekretów

Pierwszy krok jest taki sam, jak w naiwnym rozwiązaniu wyżej. To znaczy, faktycznie każdy z uczestników protokołu mnoży a_i przez b_i, otrzymując pewne g_i. Zanim przejdziemy do szczegółów kolejnego kroku, potrzebujemy jeszcze kilku oznaczeń. Oznaczmy więc wielomian $(w_a \cdot w_b)$ modulo p przez h. Wówczas wyraz wolny h to $a \cdot b$ modulo p (tak jak potrzeba), natomiast wartość $g_i = a_i \cdot b_i = w_a(y_i) \cdot w_b(y_i) = h(y_i) \pmod p$ jest znana osobie i. Problemem jest tylko stopień wielomianu

$$h(X) = (a \cdot b \bmod p) + h_1 \cdot X + h_2 \cdot X^2 + \ldots h_t X^t + \ldots h_{2t} X^{2t},$$

który wynosi $2t$. Wprowadźmy więc (trochę na siłę) nowy wielomian:

$$v(X) = (a \cdot b \bmod p) + h_1 \cdot X + h_2 \cdot X^2 + \ldots h_t X^t,$$

który powstał przez zwykłe wymazanie ostatnich t jednomianów wielomianu h. Byłoby oczywiście świetnie, gdyby osoba i potrafiła (za pomocą jakiegoś protokołu) po prostu bezpiecznie obliczyć wartość $v(y_i)$. Okazuje się, że jest to wykonalne! Co więcej, nie aż tak trudne obliczeniowo i nie wymaga dużej komunikacji między uczestnikami protokołu. Kluczowa jest tu (dość zaskakująca) obserwacja, że każde $v(y_i)$ jest kombinacją **liniową**[⋆] elementów $\{g_i\}_{i=1\ldots n}$. Gdy już to wiemy, to dalej jest z górki. Dodawanie i mnożenie przez stałą sekretów potrafimy już wykonywać. Trzeba więc tylko rozproszyć każde g_i i zastosować (być może wielokrotnie) dwa proste przypadki rozważane wyżej (oraz na koniec wysłać osobie i odpowiednie udziały do odtworzenia $v(y_i)$). Dokładne wyjaśnienie, ze względu na techniczny charakter zagadnienia, musimy niestety pominąć. Wierzymy jednak, że dokładne odtworzenie wszystkich kroków tego przypadku może być bardzo pouczające. Szczegóły znajdują się w pracy „A Full Proof of the BGW Protocol for Perfectly-secure Multiparty Computation" autorstwa Gilada Asharova oraz Yehudy Lindella.

[⋆] Czytelnik zaznajomiony z algebrą liniową oraz z pojęciem macierzy Vandermonda powinien być w stanie odtworzyć odpowiednie przekształcenie liniowe. Nie twierdzimy jednak, że jest to zadanie bardzo łatwe.

Po co to wszystko?!

Przyjmijmy, że każda z osób A_i wybrała swój własny argument $s_i \in \{0, \ldots, p-1\}$ i rozproszyła go wśród wszystkich pozostałych osób. Co umożliwiają nam protokoły naszkicowane wyżej? Otóż na pewno grupa może (wspólnie) obliczyć chociażby $s_1 + 3 \cdot s_7$ modulo p czy $s_2 + 23 \cdot s_1 \cdot s_3 \cdot s_5 + s_{100}^{44}$ modulo p (w taki sposób, że żadne obliczenia pośrednie nie są nikomu znane – wszak wszystko odbywa się dla rozproszonych wartości), bo potrafi dodawać, skalować przez stałą i mnożyć sekrety.

Gdy piszemy *grupa obliczy* $q = f(s_1, \ldots, s_n)$, to mamy na myśli, że każdy z uczestników protokołu po jego zakończeniu pozna pewne q_i takie, że wszystkie q_i razem stanowią podział q. Następnie wszyscy powinni upublicznić swoje q_i, aby każdy uczestnik mógł faktycznie poznać wartość q. Kluczową cechą tego protokołu jest, że rzeczywiście jedyną nową informacją na temat $(s_1, \ldots, s_n)$, którą pozna każdy z jego uczestników, jest właśnie q. Wszelkie informacje pośrednie pozostaną tajne.

Jak wiele w taki sposób można policzyć? Okazuje się, że ... wszystko!

Obliczenia w *ciele modulo p* mają taką cechę, że każdą funkcję (oczywiście o zbiorze wartości $\{0, \ldots, p-1\}$) da się zapisać jako wielomian, a więc jako złożenie (być może bardzo wielu) dodawań, skalowań przez stałą i mnożeń (wszystko modulo p). Innymi słowy: z faktu, że znamy protokoły dla trzech przypadków z pierwszej części artykułu, wynika, że potrafimy obliczyć zupełnie dowolną funkcję rozproszonych argumentów. Stąd już tylko krok do protokołów na np. granie w pokera przez Internet bez zaufanej strony czy bezpieczne aukcje internetowe bez serwera zbierającego i w zaufaniu porównującego oferty.

Science-fiction

Wyżej ledwie naszkicowaliśmy ideę obliczeń wielopodmiotowych (i to jeszcze w mniej ciekawym, bo pasywnym przypadku – szczegóły na jednym z marginesów). Póki co nie są one jeszcze bardzo praktyczne, ale powoli zbliżamy się do momentu, gdy (na razie) proste ich zastosowania będą możliwe do codziennego wykorzystania. Chcielibyśmy jednak mocno zaznaczyć, że drzemie w nich potencjał niemal rewolucyjny[⋆⋆].

[⋆⋆] Potencjał podobnego kalibru można wyczuć również w kilku innych pomysłach kryptologicznych, takich jak *blockchain*, *szyfrowanie homomorficzne* czy *dowody z wiedzą zerową*.

Rozpraszanie obliczeń i przechowywania danych czy ogólniej – pozbywanie się zaufanych stron z cyfrowego świata jest wszak (skromnym zdaniem autora tego tekstu) najważniejszym wyzwaniem rewolucji cyfrowej XXI wieku.