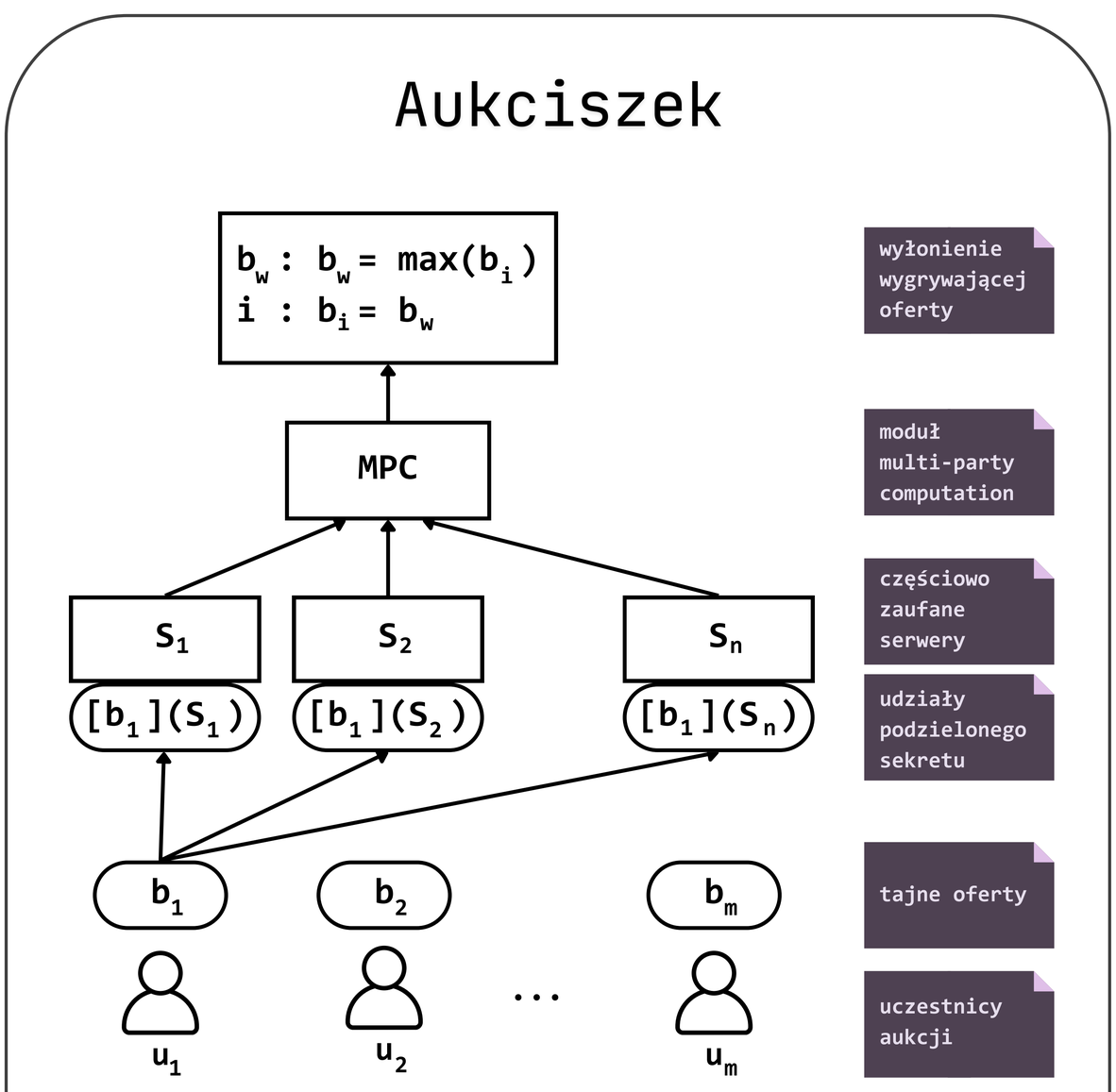
Uniwersytet im. Adama Mickiewicza w Poznaniu

Aukciszek

inż. Mateusz Piwowarski ● inż. Franciszek Czajka ● inż. Dominik Jagosz ● inż. Karol Filipiak
prof. UAM dr hab. Maciej Grześkowiak ● dr Jędrzej Garnek ● dr Jolanta Marzec-Ballesteros

Bezpieczne aukcje

Czasem przy przeprowadzeniu aukcji lub przetargów wymagane jest, aby wysokości złożonych ofert były tajne, a ogłaszana była tylko wygrywająca oferta. Strony mogą powierzyć przeprowadzenie aukcji pośrednikowi, który wybierze najlepszą z przekazanych mu propozycji. Muszą jednak bezwzględnie zaufać, że nie zdradzi on nikomu detali ich ofert.



Model logiczny systemu

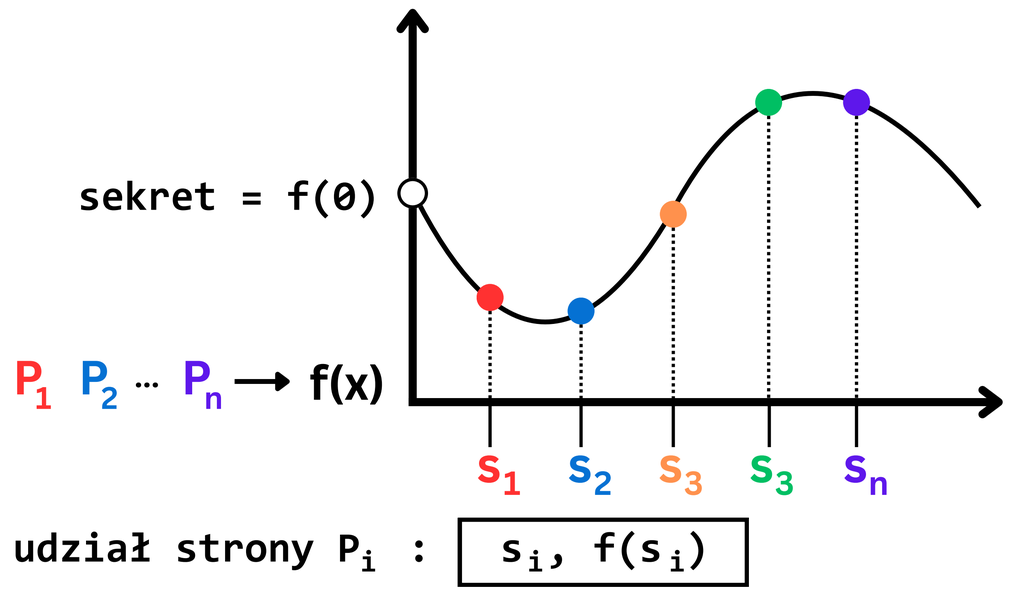
Aukciszek oferuje kryptograficzną alternatywę, która zapewnia maksymalną ochronę poufności składanych ofert. W tym celu używa metod z dziedziny multi-party computation (patrz ramka obok): schematu podziału sekretu Shamira i protokołu BGW. Proces wyboru najlepszej oferty jest zautomatyzowany i odporny na oszustwa.

Przygotowanie aukcji

Uczestnicy ustalają zbiór serwerów, na których będzie przeprowadzona aukcja. Oferta uczestnika nie będzie przesłana w całości na żaden z serwerów, ale każdy serwer będzie posiadał jej istotną część. Mówimy o zaufanej większości, jeżeli nie istnieje zmowa obejmująca więcej niż połowę serwerów (w przeciwnym wypadku nieuczciwe strony mogą złamać protokół). Dlatego wybrane serwery powinny być od siebie niezależne.

Schemat podziału sekretu Shamira

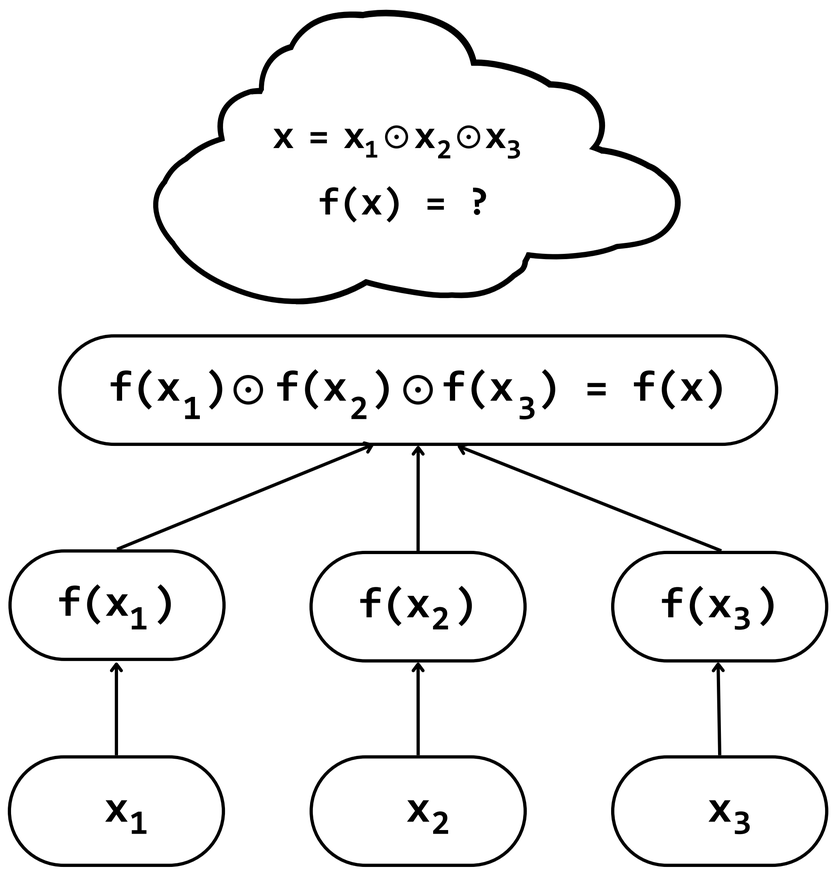
f(x) - wielomian stopnia t w Zp[X]
liczba udziałów n >= 2t + 1



udział strony P_i : $s_i, f(s_i)$

Każdy uczestnik aukcji losuje wielomian, którego wartość w punkcie 0 będzie równa wysokości jego oferty. Punkty na wielomianie stanowią udziały, które są rozdzielane pomiędzy serwery. Ujawniając co najmniej t (połowę) udziałów, można wyznaczyć wartość sekretu.

Multi-Party Computation



MPC to grupa metod, które pozwalają serwerom na obliczenie wartości funkcji na ich tajnych argumentach, bez konieczności ich ujawniania. Serwery, komunikując się ze sobą, mogą wykonywać operacje na powierzonych im sekretach, używając tylko ich udziałów. Budując schematy złożone z sum i iloczynów, można wyznaczyć wartość dowolnej funkcji. W celu rozstrzygnięcia aukcji, serwery porównują ze sobą wszystkie oferty.