Непороговое модулярное разделение секрета

Матвеев Г.В..

Схемы разделения секрета относятся к числу важных криптографических протоколов, использующихся в системах электронного голосования, шифрования на основе атрибутов, в распределенных конфиденциальных вычислениях и протоколах пороговой подписи.

Вопросы теории разделения секрета стали изучаться в НИИ ППМиИ около 15 лет тому назад. Спустя некоторое время сотрудниками института были опубликована работа.

Galibus, T. G. Matveev Generalized Mignotte's Sequences Over Polynomial Rings Electronic Notes in Theoretical Computer Science. – 2007. – Volume186. – P. 43–48. – DOI: 10.1016/j.entcs.2006.12.044.

В этой работе было предложено модулярное разделение секрета в кольце многочленов от одной переменной над полем Галуа и разработан метод реализации общей структуры доступа (GM algorithm). Тем самым было предложено непороговое модулярное разделение секрета.

Наше предложение на год опередило идентичное предложение Шнайдера патент США US20100046739A1, заявлен 22авг 2008.

Много лет спустя коллектив китайских авторов переоткрыл наш GM algorithm.

[Keju Meng](https://www.computer.org/csdl/search/default?type=author&givenName=Keju&surname=Meng), [Fuyou Miao](https://www.computer.org/csdl/search/default?type=author&givenName=Fuyou&surname=Miao) ,[Yue Yu](https://www.computer.org/csdl/search/default?type=author&givenName=Yue&surname=Yu) , [Changbin Lu](https://www.computer.org/csdl/search/default?type=author&givenName=Changbin&surname=Lu). A Universal Secret Sharing Scheme with General Access Structure Based on CRT. International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering, 2018.

В настоящее время нами выполнен цикл работ по верификации модулярного разделения секрета, протоколам пороговой подписи и изучению непорогового разделения секрета. В докладе будут затронуты следующие вопросы.

1. Трасформация пороговой схемы в непороговую с помощью GM-алгоритма.

2 .Анализ и разработка эффективных схем верификации модулярного непорогового разделения секрета.

3. Получение оценок для уровня информации модулярных реализаций непороговых структур доступа.

4. Обнаружение недобросовестных пользователей схем модулярного непорогового разделения секрета (Cheating detection).

5. Увеличение безопастного периода использования ( Life time ) частичных ключей.