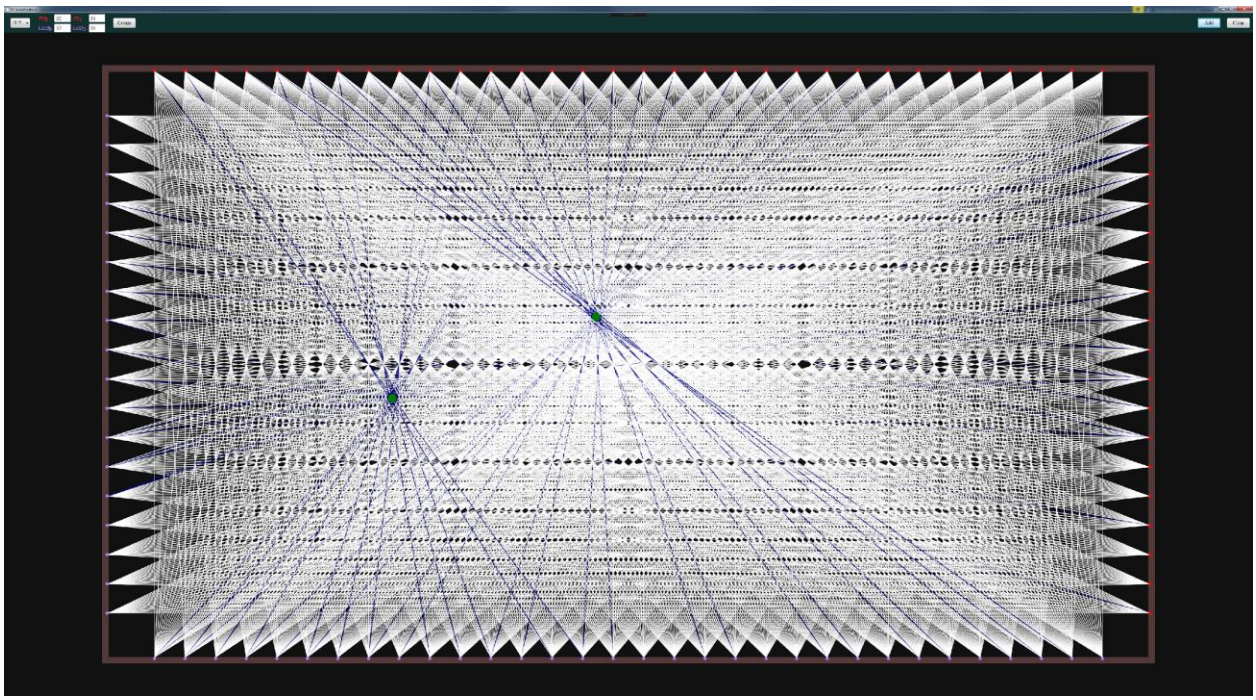

Рисунок 2 – Результат моделирования с помощью разработанного программного обеспечения

При разработке не исключается необходимость уточнения и корректировки принятых ранее решений для достижения таких характеристик как точность (не менее 3 мм) и время задержек (не более 20 мс) [3].

Список использованных источников:

1. Актуальные проблемы энергетики – 2016: материалы науч.-техн. конф. студентов и аспирантов, Минск, 2017 г. / Белорус. нац. технический ун-т; редкол.: Т. Е. Жуковская [и др.]. – Минск : БНТУ, 2017. – 537 с.
2. Google Patents [электронный ресурс] / Infrared ray touch panel device with high efficiency. – 2019. – Режим доступа: https://patents.google.com/patent/US20110175848A1/en?oq=US20110175848A1. – Дата доступа: 15.03.2019.
3. Vasuki, S. An interactive infrared sensor based multi-touch panel / S. Vasuki, P. Mordhwaj, N. Rounak Singh // International Journal of Scientific and Research Publications – 2013. – Vol. 3, № 3. – ISSN 2250-3153.

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ НА БАЗЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Коминч В.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Станкевич А.В. – к.т.н.,доцент

Защита интеллектуальной собственности является одной из самых важных проблем века информации. Для решения данной проблемы специалистами были разработаны различные алгоритмы электронной цифровой подписи. В докладе рассматривается аппаратная реализация на базе ПЛИС белорусского стандарта СТБ 34.101.45 – 2013, который представляет собой алгоритм электронной цифровой подписи на эллиптических кривых.

Входными параметрами алгоритма генерации цифровой подписи СТБ 34.101.45 являются входное сообщение произвольной длины и личный (секретный) ключ. Кроме того, на вход алгоритма также подаются параметры эллиптической кривой: уровень стойкости, коэффициенты кривой, порядок группы, базовая точка. По модулю порядка группы определяется уровень стойкости. Выходным параметром является цифровая подпись.

В качестве эллиптической кривой над конечным полем Fp используется следующее уравнение:

$y^2 = x^3 + a * x + b \ (mod\ p)$, где p - большое простое число.

Совокупность точек, удовлетворяющих уравнению, образует конечное поле. Над этим полем реализованы такие операции, как сложение и умножение на константу (вычисляется через многократное суммирование). С операцией умножения на константу связана основная задача по взлому таких кривых. Она носит название задачи дискретного логарифмирования. Её суть

заключается в подборе того коэффициента, на который умножали базовую точку. Именно этот коэффициент является закрытым ключом.

На рисунке 1 представлена структурная схема устройства для генерации цифровой подписи. В случае использования стандартной эллиптической кривой схему можно упростить, убрав генератор параметров эллиптической кривой и подавая на вход блоков электронной подписи соответствующие параметры.

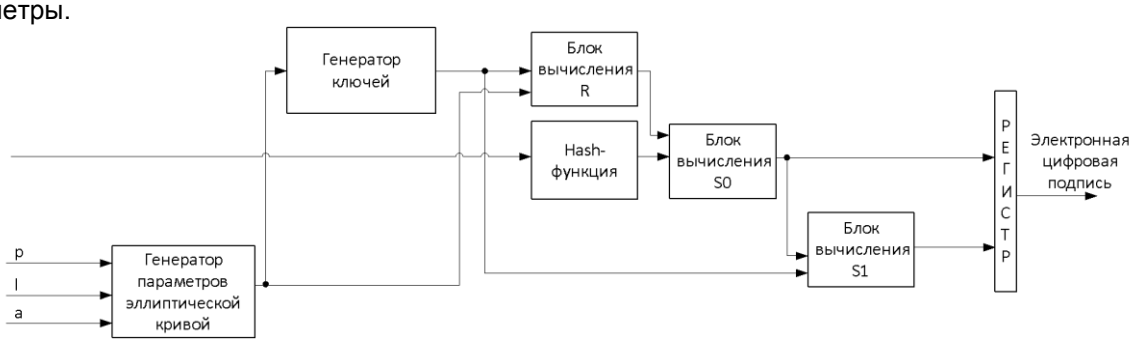

Рисунок 1 – Структурная схема устройства для выработки электронной цифровой подписи

$R = k * G$, где G – базовая точка, являющаяся выходом генератора параметров эллиптической кривой. Блоки S0 и S1 являются частями итоговой подписи и выражаются следующими формулами:

$S_0 =< belt - hash(OID(h)|| < R >_{2l} ||H) >_l$,

$S_1 =< (k - \underline{H} - \left(\underline{S_0} + 2^l\right) d \ mod \ q) >_{2l}$, где belt-hash – функция хэширования, H – выход блока хэш-функции, OID – идентификатор функции($06092A7000020022651F51_{16}$), R – выход блока вычисления R, d – личный ключ, q – порядок группы точек из поля Fp.

Уровень стойкости равен 128. Длина итоговой подписи равна 384 бита.

Одним из блоков алгоритма электронной цифровой подписи является блок вычисления функции хэширования. В качестве функции хэширования выбрана функция из стандарта СТБ 34.101.31-2011, в основе вычисления которой лежит алгоритм блочного шифрования из того же стандарта. При использовании данной хэш-функции в алгоритме электронной цифровой подписи на ее вход подается сообщение фиксированной длины. На выходе функции получается хэш-значение длиной 256 бит.

Приведенное устройство реализуется на базе FPGA семейства Virtex 7 фирмы Xilinx.

Аппаратную реализацию цифровой подписи можно использовать для проверки транзакций криптовалют, цифровых операций с валютами (платежами), подписи на электронные документы и любые другие файлы.

Список использованных источников:

1. Информационные технологии. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых : СТБ 34.101.45–2013. – Введ. 30.08.201. – Минск : Госстандарт, 2013. – 41 с.

УСТРОЙСТВО ДЛЯ НЕПРЕРЫВНОГО НЕИНВАЗИВНОГО ИЗМЕНЕНИЯ АРТЕРИАЛЬНОГО ДАВЛЕНИЯ

Крылов Н.Д.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Азаров И.С. – д.т.н.,доцент

Развитие микроэлектроники и элементной базы позволило выйти носимой электронике на новый уровень. Однако ряд актуальных задач остается нерешенным. Одной из таких задач является непрерывное неинвазивное измерение артериального давления. Решить данную задачу призваны алгоритмы машинного обучения.

На сегодняшний день измерение артериального давления вне реанимации производится методом Короткова, что доставляет дискомфорт пациенту и не позволяет производить непрерывное измерение. Решение данной проблемы возможно при измерении давления по косвенным признакам. Наиболее точным методом является измерение методом допплерографии, однако такой подход является технически сложным, дорогим и менее исследованным. Альтернативным подходом является анализ кривой фотоплетизмограммы (далее PPG). Существуют исследования[1-3],