# Резюме по статье «Fast Variants of RSA»

В своей работе авторы статьи отмечают значимость и распространенность криптосистемы RSA, а также её главный недостаток – недостаточно быструю работу. В статье предлагается 4 варианта решения это проблемы, причем все варианты являются обратно совместимыми, то есть способными взаимодействовать со стандартной реализацией RSA.

Batch RSA или «пакетный» RSA – модификация стандартного алгоритма, при котором можно расшифровать два шифртекста примерно по цене одного, при условии что в открытых ключах и , а и малы. Для этого нужно вычислить , но данную операцию можно привести к виду , что позволяет уменьшить количество операций взятия корня до одной. Данный способ позволяет достичь увеличения скорости до 3 раз, но требует очень маленьких открытых показателей

Вторая модификация – Multi-prime RSA или RSA с несколькими простыми. Основная суть данной модификации заключается в использовании вместо двух больших простых чисел b простых чисел меньшей размерности. Прирост производительности осуществляется за счет снижения сложности операции возведения в степень по модулю. Так, в классической реализации используется возведение в степень по модулю -разрядных чисел. В данной модификации берется модуль по модулю -разрядных чисел. Данное нововведение дает прирост производительности в 2 и более раз, в зависимости от n. Стоит отметить, что в случае 1024-разрядного n простых чисел в целях безопасности можно взять только 3, то есть .

Третья модификация схожа со второй, и относится к той же группе. Multi-factor RSA или RSA с несколькими степенями. Суть модификации идентична предыдущей, но в данном варианте выбирается не b различных простых чисел длины , а и , причем берется раз, то есть . Таким образом дешифрования требует двух возведений в степень по модулю битных чисел и поднятий Хензеля. Данный способ дает прирост производительности примерно в 3 раза.

Последней модификацией является Rebalanced RSA или перебалансированный RSA. Основная идея данной модификации состоит в уменьшении времени дешифрования за счет увеличения времени шифрования. В данном методе выбирается так, чтобы оно было порядка , но при том и были малыми числами. Это позволяет в КТО заменить показатель на -разрядные числа, где сравнительно мало. Прирост производительности при таком подходе порядка 3 раз.