# Cryptology ePrint Archive: Report 2011/024

**Secure evaluation of polynomial using privacy ring homomorphisms**

*Alexander Rostovtsev, Alexey Bogdanov and Mikhail Mikhaylov*

**Abstract:** Method of secure evaluation of polynomial y=F(x_1, …, x_k) over some rings on untrusted computer is proposed. Two models of untrusted computer are considered: passive and active. In passive model untrusted computer correctly computes polynomial F and tries to know secret input (x_1, …, x_k) and output y. In active model untrusted computer tries to know input and output and tries to change correct output y so that this change cannot be determined. Secure computation is proposed by using one-time privacy ring homomorphism Z/nZ -> Z/nZ[z]/(f(z)), n = pq, generated by trusted computer. In the case of active model secret check point v = F(u_1, …, u_k) is used. Trusted computer generates polynomial f(z)=(z-t)(z+t), t in Z/nZ, and input X_i(z) in Z/nZ[z]/(f(z)) such that X_i(t)=x_i (mod n) for passive model, and f(z)=(z-t_1)(z-t_2)(z-t_3), t_i in Z/nZ and input X_i (z) in Z/nZ[z]/(f(z)) such that X_i(t_1)=x_i (mod n), X_i(t_2)= u_i (mod n) for active model. Untrusted computer computes function Y(z) = F(X_1(z), …, X_k(z)) in the ring Z/nZ[z]/(f(z)). For passive model trusted computer determines secret output y=Y(t) (mod n). For active model trusted computer checks that Y(t_2)=v (mod n), then determines correct output y=Y(t_1) (mod n).

**Category / Keywords:** cryptographic protocols / elliptic curve cryptosystem, factoring, public-key cryptography

**Date:** received 12 Jan 2011

**Contact author:** rostovtsev at ssl stu neva ru