

Introduction

There is no systematic approach to assessing security of public key cryptosystems.

Experiment to assess security of AAG cryptosystem..

Length based attacks work but are not well understood.

Computer experiments produce data on efficacy of length based attacks.

Modify AAG as suggested by experimental results and test new system.

Test diffusion.

Results

Length based attack is now understood.

Modified AAG resists all known attacks, and may also resist quantum attacks.

Lack of diffusion is a potential risk, as illustrated below.



Computed public key reveals private key.



Diffuse by free reduction.



By Dehornoy normal forms.



By approximate geodesics.