On the Security of a Variant of ElGamal Encryption Scheme

ABSTRACT

NOWADAYS, huge amounts of personal data are generated and collected everywhere due to the rapid advancement of technologies. The use of machine learning techniques makes it possible to extract useful knowledge from these data. However, because of their sensitivity, it is critical that such data be strongly protected by using encryption not only for the data at rest but also when performing analytics on the data. Recent cryptosystems with homomorphic properties have made possible to perform computations over ciphertexts. Two very well-known public-key cryptosystems with homomorphic properties are the ElGamal and Paillier's cryptosystems. Both are considered *partially* homomorphic cryptosystem since given any two ciphertexts, they support the generation of a ciphertext associated with either the addition or the multiplication of the two underlying plaintexts, but not both.

EXISTING SYSTEM

Recently, based on the Paillier cryptosystem proposed a distributed ElGamal cryptosystem which allows for both a much simpler distributed key generation procedure and distributed decryption of messages from a large plaintext domain. Both are considered *partially* homomorphic cryptosystem since given any two ciphertexts, they support the generation of a ciphertext associated with either the addition or the multiplication of the two underlying plaintexts, but not both. Hence, to enable practical privacy-preserving analyses of the data encrypted by a public-key homomorphic encryption scheme, current solutions usually involve the distribution of the private key into multiple shares among.

Disadvantages

- Insecurity of the variant of encryption based on the Paillier encryption scheme.
- Approach for distributed key generation is fairly complex and the cost of distributed decryption is still at least three times higher than that of centralized decryption in that the shares of the private key have to be long enough to properly hide the private key from those participants.

PROPOSED SYSTEM

In this paper, a feasible attack against a variant of ElGamal encryption scheme recently proposed has been shown. Any adversary having access to the prime order of the underlying group in the ElGamal encryption scheme would be able to mount such an attack, which results in the total exposure of the secret key in the distributed cryptosystem.

Advantages

- ElGamal encryption scheme and show a feasible attack allowing an attacker to derive the private key given the prime order of the underlying group.
- ElGamal encryption scheme supporting efficient distributed key generation and distributed decryption.

SOFTWARE REQUIREMENTS

Front-end	:	JSP
Back-End	:	MySQL
Server	:	Tomcat Server
OS	:	WINDOWS 7/above

HARDWARE REQUIREMENTS

PROCESSOR	:	CORE i3
RAM	:	512MB-2GB
HARD DISK	:	40GB