International Journal of Pure and Applied Mathematics
Volume 83 No. 5 2013, 635-638
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v83i5.4

CRYPTANALYSIS OF PUBLIC-KEY CRYPTOSYSTEMS AND DIGITAL SIGNATURES

Debasis Giri
Department of Computer Science Engineering
Haldia Institute of Technology
Haldia-721657, India

Invited Talk
NCRTMSA – 2012

*

Cryptographic protocols play a major role in many applications where data integrity, confidentiality, authenticity and other security-related issues are crucial. Out of these protocols, the most important and widely studied are confidentiality and authenticity. Confidentiality and authenticity can be done through encryption and digital signature respectively. Encryption and Digital signature are some fundamental cryptographic primitives which are useful for stand-alone applications and for building a variety of security protocols. To design cryptographic protocols are not enough, their security guarantee is also paramount importance. Therefore, in this report, security weaknesses are identified for some protocols [4, 11, 12]. We then describe some security protocols for encryption of long confidential message [1] based on RSA cryptosystem and then describe security analysis of these protocols [5, 6, 7].

We then describe variety digital signatures, like proxy signature [2] (which is based on Bilinear Pairings) and multi-signature [3] (which is based on composite

modulus) and then describe their security [5, 8, 10, 9]. In the following, we only describe an existing security protocols for multi-signature citeDGiri3.

Multi-Signature Scheme. We describe the different phases of the scheme below:

Setup Procedure. The GCSs select two large primes p and q. The GCSs select an integer g, $1 < g < pq$ such that order of g is large. Let $(\alpha_i, x_i = g^{\alpha_i} \bmod pq)$ be the private/public key pair of a member M_i.

Partial Signatures Generation. Suppose a group consists of n number of members M_i $(i = 1, 2, \ldots, n)$. Each member M_i chooses a random number r_i, computes $t_i = g^{r_i} \bmod pq$ and broadcasts t_i. Further, each GCS_j $(j = 1, \ldots, v)$ chooses a random number r_{GCS_j}, computes $t_{GCS_j} = g^{r_{GCS_j}} \bmod pq$ and broadcasts it. These broadcasted messages t_i, $i = 1, 2, \ldots, n$ and t_{GCS_j}, $j = 1, 2, \ldots, v$ must be accompanied by digital signatures on these by its individual sender so that other members of the group can verify the identity of the sender. Each member of the group and each GCS can compute $t = \prod_{i=1}^{n} t_i \cdot \prod_{j=1}^{v} t_{GCS_j} \bmod pq$. Each member M_i then generates partial signature on the message m as follows:

1. Compute $s_i = H(m, t)\alpha_i + r_i$.
2. Transmit the pair (s_i, m) as partial signature on m to the GCS to which M_i is connected.

On receiving (s_i, m) from M_i, the GCS checks the validity of the partial signature on m from the following condition $g^{s_i} = x_i^{H(m,t)} t_i \bmod pq$. If the above condition is true, the partial signature on m is valid; otherwise it becomes invalid.

Partial Signatures Aggregation. After validation of all partial signatures, the GCS generates a multisignature on the message as follows:

1. Compute $s_0 = H(m, t)\alpha_0 + \sum_{j=1}^{v} r_{GCS_j} \bmod (p-1)(q-1)$.
2. Compute $s = \sum_{i=0}^{n} s_i \bmod (p-1)(q-1)$.
3. Transmit multisignature (s, t) on the message m to all member of the group.

After receiving (s, t) from the GCS, each member of the group checks the validity from the following condition $g^s = x^{H(m,t)} t \bmod pq$, where $x = \prod_{i=0}^{n} x_i \bmod$

pq. If the condition is true, he confirms that the multisignature is valid; otherwise it is treated as invalid.

Our protocol is summarized below:

We conclude that attacking a scheme is difficult, provided some problems from number theory is hard to solve.

References

[1] Debasis Giri, Prithayan Barua, P.D. Srivastava, Biswapati Jana, A cryptosystem for encryption and decryption of long confidential messages, In: *4-th International Conference on Information Security and Assurance (ISA 2010), Information Security and Assurance Communications in Computer and Information Science*, **76** (2010), 86-96.

[2] Debasis Giri, P.D. Srivastava, An improved efficient multisignature scheme in group communication systems, In: *15-th International Conference on Advanced Computing & Communication (ADCOM 2007)*, IEEE Computer Society (2007), 447-453.

[3] Debasis Giri, P.D. Srivastava, Cryptanalysis and improvement of Das et als proxy signature scheme, In: *10-th International Conference on Information Technology (ICIT 2007)*, IEEE Computer Society (2007), 151-154.

[4] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, **21**, No. 2 (1978), 120-126.

[5] M. Bellare, P. Rogaway, Random oracles are practical: A paradigm for designing efficient protocols, In: *Proceedings of First ACM Conference on Computer and Communications Security* (1993), 62-73.

[6] M. Bellare, P. Rogaway, Optimal asymmetric encryption, In: *Advances in Cryptology -Proceedings of Eurocrypt'94*, Springer-Verlag(LNCS), **950** (1994), 92-111.

[7] R. Cramer, V. Shoup, A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack, *Advances in Cryptology - Proceedings of CRYPTO'98*,Springer-Verlag (LNCS), **1462** (1998), 13-25.

[8] V. Varadharajan, P. Allen, S. Black, An analysis of the proxy problem in distributed systems, In: *In Proceedings of 1991 IEEE Computer Society Symposium on Research in Security and Privacy* (1991), 255-275.

[9] Z. Shao, Proxy signature schemes based on factoring, *Information Processing Letters*, **85**, No. 3 (2003), 137-143.

[10] K. Ohta, T. Okamoto, Multisignature schemes secure against active insider attacks, *IEICE Transactions on Fundamentals*, *E82-A* (1999), 21-31.

[11] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory*, **31**, No. 4 (1985), 469-472.

[12] Z. Shao, Signature Scheme based on discrete logarithm without using one-way hash functions, *Electronics Letters*, **34**, No. 11 (1978), 1079-1080.