2009 International Conference on Networks Security, Wireless Communications and Trusted Computing

Security Difference Between DSA and Schnorr's Signature

Zhengjun Cao[1,2] Olivier Markowitch[2]
1 Department of Mathematics, Shanghai University, China
2 Computer Sciences Department, Université Libre de Bruxelles, Belgium
Email: caozhj@yahoo.cn zhencao@ulb.ac.be

Abstract

We investigate the security difference between DSA and Schnorr's signature. The security of DSA can be reduced to the problem: to find $m \in \Omega, \rho, \theta \in \mathcal{Z}_q^*$ such that $\mathcal{H}(m) = \rho\left((g^\rho y)^\theta \bmod p\right) \bmod q$, where Ω denotes the text space and the message m is not restrained. Unlike DSA evaluates the hash function only at the message m, Schnorr's signature adopts a self-feedback mode by evaluating the hash function at (m, r, s). Thus its security becomes more robust.

1. Introduction

In 1984, ElGamal [2] proposed a famous cryptographic mechanism, which can be used for both digital signatures and encryption. The ElGamal mechanism gets its security from the difficulty of calculating discrete logarithms in a finite field. In the past two decades, many variations of the ElGamal signature have been proposed, including DSA and Schnorr's signature [10]. Schneier [9] claimed that DSA is not a derivative of the Schnorr's signature, nor even of ElGamal's signature. All three are examples of the general construction of discrete-logarithm-based digital signatures. A question should then be raised. Are all the variants equally secure?

Notice that there is a marked difference between many variations of the ElGamal signature and Schnorr's signature. Now we only use DSA to illustrate this difference. See the following table.

	Verification
DSA	$r = (g^{\mathcal{H}(m)s^{-1}} y^{rs^{-1}} \bmod p) \bmod q.$
Schnorr's signature	$r = \mathcal{H}(m \| g^s y^{-r} \bmod p)$

Table 1. DSA and Schnorr's signature

Clearly, the Schnorr's signature evaluates the hash function at the resulting signature (m, r, s) rather than DSA evaluates it just at m.

In 1996, Vaudenay [12] introduced hidden collision attacks against DSA based on forging public parameters. In 2005, Wang et al [14] presented a collision attack against the hash function SHA-1. But the resulting texts m_1, m_2, satisfying SHA-1$(m_1) =$ SHA-1(m_2), are usually restrained.

In this paper, we investigate the security difference between DSA and Schnorr's signature. Our results show that the security of DSA can be reduced to the problem, to find a triple $m \in \Omega, \rho, \theta \in \mathcal{Z}_q^*$ such that $\mathcal{H}(m) = \rho\left((g^\rho y)^\theta \bmod p\right) \bmod q$, where Ω denotes the text space. Compared with the common temporary key-only attack, to find $r, k \in \mathcal{Z}_q^*$ such that $r = (g^k \bmod p) \bmod q$, where $r \in \mathcal{R}$, $\mathcal{R}$ denotes the set of those legal r's issued by the signer using the same secret key x, the new attack is more effective because of the big length gap between $|p|$ (1024-bit) and $|q|$ (160-bit). If $\rho\,(\neq 1)$ is settled in advance, the running time of the new attack is $O(\sqrt{\frac{q}{|\mathcal{S}^{(m)}|}})$, where

$$\mathcal{S}^{(m)} \overset{\text{def}}{=} \left\{\hat{g}^t \bmod p : 0 < t \leq q-1, \hat{g} = g^\rho y \bmod p\right\} \bigcap$$

$$\left\{z + iq : 0 \leq i \leq \left[\frac{p-z}{q}\right], z = \mathcal{H}(m)\rho^{-1} \bmod q, m \in \Omega\right\}$$

But Schnorr's signature is free of the new attack because it uses a self-feedback mode. More precisely, it evaluates the hash function at (m, r, s) rather than DSA evaluates it only at the message m.

2. Description of DSA

The signature mechanism requires a hash function $\mathcal{H} : \{0,1\}^* \longrightarrow \mathcal{Z}_q^*$ for some integer q. The DSS explicitly requires use of the Secure Hash Algorithm (SHA-1). It's universally believed that the security of DSA relies on two distinct but related discrete logarithm problems. One is the logarithm problem in $\mathcal{Z}_p^*$. The other is the logarithm problem in the cyclic subgroup of order q.

[Public key] p : 512-bit to 1024-bit prime. q : 160-bit prime factor of $p-1$. g : a base element of order q mod p. $y := g^x \bmod p$.

[Private Key] $x \in \mathcal{Z}_q^*$ (a 160-bit number).

[Signing] (1) Select a random secret integer $k \in \mathcal{Z}_q^*$. (2) Compute $r = (g^k \bmod p) \bmod q$, $s = k^{-1}(\mathcal{H}(m) + xr) \bmod q$. (3) The signature for message m is the pair (r, s).

[Verifying] Accept it if and only if

$$(g^{\mathcal{H}(m)s^{-1}} y^{rs^{-1}} \bmod p) \bmod q = r$$

where s^{-1} is computed in $\mathcal{Z}_q^*$.

978-0-7695-3610-1/09 $25.00 © 2009 IEEE
DOI 10.1109/NSWCTC.2009.141

3. Common attacks

It's well-known that there are two common attacks against DSA.

(1) Key-only attack against k or x. We know each signature requires a new value of k, and the value must be chosen randomly. If Eve ever recovers a k that Alice used to sign a message, perhaps by exploiting some properties of the random-number generator that generated k, she can recover Alice's private key x. If Eve ever gets two messages signed using the same k, even if she doesn't know what it is, she can recover x. And with x, Eve can generate undetectable forgeries of Alice's signature. In any implementation of the DSA, a good random-number generator is essential to the system's security.

(2) Collision attack against the hash function SHA-1 used in DSA.

A complete description of "key-only attack against k" can be specified as follows:

1. Given a signature (r, s) on a message m, find k such that $r = (g^k \bmod p) \bmod q$.
2. From k, recover the private key $x = (ks - H(m))/r \bmod q$.

As for other attacks against DSA, we refer to [13], [12].

4. The attack against k versus the attack against x

It should be stressed that there is a marked difference between the attack against the temporary k and the secret key x. Actually, the attack against k does surpass the attack against x.

The attack against k aims at finding $r \in \mathcal{R}, k \in \mathcal{Z}_q^*$ such that

$$r = (g^k \bmod p) \bmod q \tag{1}$$

where $\mathcal{R}$ denotes the set of those legal r's issued by the signer using the same secret key x. In nature, it is equivalent to

$$g^k \bmod p = \begin{cases} r \\ r+q \\ \vdots \\ r + \left[\frac{p-r}{q}\right] q \end{cases}$$

Compared with the common key-only attack, to find $x \in \mathcal{Z}_q^*$ such that

$$y = g^x \bmod p \tag{2}$$

the attack against k is more effective because of the big length gap between $|p|$ (1024-bit) and $|q|$ (160-bit). Roughly speaking, the length gap of two modulus results in an increase of the number of solutions to Eq.(1). The running time of the attack against x using Pollard's rho algorithm is $O(\sqrt{q})$. However, the running time of the attack against k is $O(\sqrt{\frac{q}{|\mathcal{S}_{(r)}|}})$ using Pollard's rho algorithm for a fixed r, where

$$\mathcal{S}_{(r)} \overset{\text{def}}{=} \left\{g^t \bmod p \,:\, 0 < t \leq q-1\right\} \bigcap$$

$$\left\{r + iq \,:\, 0 \leq i \leq \left[\frac{p-r}{q}\right]\right\}$$

In fact, without loss of generality, we assume that the $|\mathcal{S}_{(r)}|$ solutions to Eq.(1) are uniformly distributed in the interval $[0, q-1]$. If we equally divide the interval into $|\mathcal{S}_{(r)}|$ intervals, then there is a unique solution to Eq.(1) in each interval, which is of the length $\frac{q}{|\mathcal{S}_{(r)}|}$.

Considering r may be chosen from those legal signatures issued by the signer using the same secret key x, the attack against k is more effective. The running time of the attack against k using Pollard's rho algorithm is $O(\sqrt{\frac{q}{|\mathcal{S}^{(r)}|}})$, where

$$\mathcal{S}^{(r)} \overset{\text{def}}{=} \left\{g^t \bmod p \,:\, 0 < t \leq q-1\right\} \bigcap$$

$$\left\{r + iq \,:\, 0 \leq i \leq \left[\frac{p-r}{q}\right], r \in \mathcal{R}\right\}$$

5. An attack against DSA based on the length gap of two modulus

5.1. Basic idea

By the verification in DSA, we have:

$$r = \left(g^{\mathcal{H}(m)s^{-1}} y^{rs^{-1}} \bmod p\right) \bmod q$$

Suppose that $\quad r = \left(g^{\alpha} y^{\beta} \bmod p\right) \bmod q$
and set

$$\begin{cases} (g^{\alpha}y^{\beta})^s = g^{\mathcal{H}(m)} y^{(g^{\alpha}y^{\beta} \bmod p)} \bmod p \\ \alpha s = \mathcal{H}(m) \bmod q \\ \beta s = (g^{\alpha}y^{\beta} \bmod p) \bmod q \end{cases}$$

Thus, $\mathcal{H}(m) = \alpha\beta^{-1}\left(g^{\alpha}y^{\beta} \bmod p\right) \bmod q$.

Denote the text space by Ω. To launch an attack against DSA, it suffices to find $\alpha, \beta \in \mathcal{Z}_q^*$ and $m \in \Omega$ such that

$$\mathcal{H}(m) = \alpha\beta^{-1}\left(g^{\alpha}y^{\beta} \bmod p\right) \bmod q \tag{3}$$

and compute

$$r = \left(g^{\alpha}y^{\beta} \bmod p\right) \bmod q, \qquad s = r\beta^{-1} \bmod q$$

The resulting signature is (m, r, s).

5.2. The new attack versus the key-only attack against k

We claim that Eq.(3) is less intractable than Eq.(1). In fact, the Eq.(3) is reduced to

$$\mathcal{H}(m) = \rho\left((g^\rho y)^\beta \,\mathrm{mod}\, p\right) \,\mathrm{mod}\, q$$

if we take $\alpha = \rho\beta \,\mathrm{mod}\, q$ and settle $\rho\,(\neq 1)$ in advance. Since the order of g relative to p is q and $y = g^x \,\mathrm{mod}\, p$, the above equation can be written as

$$\mathcal{H}(m) = \rho\left(\hat{g}^\beta \,\mathrm{mod}\, p\right) \,\mathrm{mod}\, q$$

where $\hat{g} = g^\rho y \,\mathrm{mod}\, p$, $\mathrm{Ord}_p(\hat{g}) = q$. Thus we consider the following problem, to find $\theta \in \mathcal{Z}_q^*$ and $m \in \Omega$, given ρ, p, q, such that

$$\mathcal{H}(m)\rho^{-1} = \left(\hat{g}^\theta \,\mathrm{mod}\, p\right) \,\mathrm{mod}\, q \qquad (4)$$

For a fixed $\rho \in \mathcal{Z}_q^*$, we define the following set

$$\mathcal{S}^{(m)} \overset{\text{def}}{=} \left\{\hat{g}^t \,\mathrm{mod}\, p \;:\; 0 < t \le q-1, \hat{g} = g^\rho y \,\mathrm{mod}\, p\right\} \bigcap$$

$$\left\{z + iq \;:\; 0 \le i \le \left[\frac{p-z}{q}\right],\, z = \mathcal{H}(m)\rho^{-1} \,\mathrm{mod}\, q,\, m \in \Omega\right\}$$

Notice that $\mathrm{Ord}_p(\hat{g}) = q = \mathrm{Ord}_p(g)$, thus

$$\left\{\hat{g}^t \,\mathrm{mod}\, p \;:\; 0 < t \le q-1\right\} = \left\{g^t \,\mathrm{mod}\, p \;:\; 0 < t \le q-1\right\}$$

Recall that

$$\mathcal{S}^{(r)} = \left\{g^t \,\mathrm{mod} p \,:, 0 < t \le q-1\right\}$$

$$\bigcap\left\{r + iq : 0 \le i \le \left[\frac{p-r}{q}\right], r \in \mathcal{R}\right\}$$

and the set $\mathcal{R}$ consists of those legal r's issued by the signer using the same secret key x, we have

$$|\mathcal{S}^{(m)}| \ge |\mathcal{S}^{(r)}|$$

because it's always reasonable to assume $|\Omega| >> |\mathcal{R}|$ in practice. It's easy to find that the number of solutions to Eq.(4) is $|S^{(m)}|$. Therefore, the running time of this collision attack is $O(\sqrt{\frac{q}{|\mathcal{S}^{(m)}|}})$.

5.3. Further discussion

We know the collision attack against the hash function SHA-1 [14] is an excellent work in recent. But the resulting texts m_1, m_2 satisfying SHA-1(m_1) = SHA-1(m_2) are usually restrained. The key-only attack against k is of little efficiency because r is restrained. However, the new attack is of more practical significance since the text m is not restrained.

The cardinal of $S^{(m)}$ (see the above definition) is of great importance in practice. Regretfully, it seems that it is difficult to make a positive or negative theoretical analysis of it. In the collision attack, we can also define

$$\mathcal{S}^{(m,\rho)} \overset{\text{def}}{=} \left\{(g^\rho y)^t \,\mathrm{mod} p : 0 < t \le q-1, \rho \in \mathcal{Z}_q^*\right\}$$

$$\bigcap\{z + iq : 0 \le i \le \left[\frac{p-z}{q}\right],$$

$$z = \mathcal{H}(m)\rho^{-1} \,\mathrm{mod} q, \rho \in \mathcal{Z}_q^*, m \in \Omega\}$$

if we do not fix ρ in advance. Under the circumstance, the number of solutions to the collision problem in DSA is $|\mathcal{S}^{(m,\rho)}|$.

6. Schnorr's signature and its self-feedback mode

Historically, many researchers believed that DSA was very similar to the Schnorr's signature. It consequently led to a lawsuit [3]. In this section, we will definitely point out that Schnorr's signature is free of the new attack because it uses a self-feedback mode. An adversary cannot disassemble computational assignments for finding similar collisions. In this regard, Schnorr's signature is more robust than DSA.

6.1. Description

It's well known that DSA is related to Schnorr's signature. The signature scheme employs a subgroup of order q in $\mathcal{Z}_p^*$, where p is a large prime number. It also requires a hash function $\mathcal{H} : \{0,1\}^* \longrightarrow \mathcal{Z}_q$.

[Setup] Public key: p, a large prime. q, a large prime factor of $p-1$. g, a base element of order q mod p. $y =\; g^x$ mod p. Private Key: $x \in \mathcal{Z}_q^*$.

[Signing] (1) Select a random secret integer $k \in \mathcal{Z}_q^*$. (2) Compute $e = g^k$ mod p, $r = \mathcal{H}(m||e)$, $s = xr + k$ mod q. (3) The signature for message m is the pair (r, s).

[Verifying] Accept it if and only if

$$\mathcal{H}(m||g^s y^{-r} \,\mathrm{mod}\, p) = r$$

6.2. An advantage

A marked difference between DSA and Schnorr's signature is that the resulting signature (r, s) in the latter should be input into the hash function $\mathcal{H}(\cdot)$ for verification. But in DSA the hash function $\mathcal{H}(\cdot)$ evaluates only at the message m. In other words, Schnorr's signature uses a self-feedback mode. Thus an adversary is forced to search for a digest r so that

$$\mathcal{H}(m||g^s y^{-r} \,\mathrm{mod}\, p) = r \quad \text{for given } p, g, y, \mathcal{H}(\cdot) \qquad (5)$$

According to some general cryptographic assumptions on $\mathcal{H}(\cdot)$, the problem is very intractable.

The challenge in (5) is introduced in Schnorr's signature. In the signature scheme, the resulting r is tightly bound with the given message m and another signature datum s. An adversary cannot disassemble computational assignments because the output and input of $\mathcal{H}(\cdot)$ should be generated *synchronously*. Regretfully, neither r nor s in DSA is bound to m in this way. In short, Schnorr's signature is more closely related to DLP than DSA [7], [8], [11], [6].

7. Conclusion

The exponent q has a comparatively short length (160-bit), while the modulus p is of 1024-bit length. In 2004, Koblitz and Menezes [4] remarked that:

> The reductionist security failure is a much more serious matter than any of the issues that the anti-DSA people raised in 1992 [1]. It is also surprising that apparently none of the NSA cryptographers noticed this possible objection to DSA. If they had, they could have easily fixed it (without any significant loss of efficiency) by having the signer evaluate the hash function at (m, r) rather than just at m.

Intuitively, if the signer evaluates the hash function at (m, r) rather than just at m, the security of DSA becomes more robust.

Acknowledgement

Supported by National Natural Science Foundation of China (Project 60873227), Cryptasc Project (Institute for the encouragement of Scientific Research and Innovation of Brussels), Innovation Program of Shanghai Municipal Education Commission, Shanghai Leading Academic Discipline Project (J50101), Key Disciplines of Shanghai Municipality (S30104).

References

[1] D. Branstad, M. Smid. Responses to comments on the NIST proposed digital signature standard, In: *Advances in Cryptology CRYPTO'92*, Lectures Notes in Computer Science 740, pp. 76-88. Springer-Verlag, 1992.

[2] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms, In: *Advances in Cryptology CRYPTO'84*, Lectures Notes in Computer Science 196, pp. 10-18. Springer-Verlag, 1984.

[3] http://www.ibiblio.org/patents/txt/crypt.txt

[4] N. Koblitz, A. Menezes. Another look at provable security, *Journal of Cryptology*, Vol. 20, 1, pp. 3-37. Springer-Verlag, 2007.

[5] A. Menezes, P. Oorschot, S. Vanstone. *Handbook of Applied Cryptography*, CRC Press, 1996.

[6] P. Paillier, D. Vergnaud. Discrete-log-based signatures may not be equivalent to discrete log. In: *Advances in Cryptology ASIACRYPT 2005*, Lectures Notes in Computer Science 3788, pp. 1-20. Springer-Verlag, 2005.

[7] D. Pointcheval, J. Stern. Security proofs for signature schemes, In: *Advances in Cryptology EUROCRYPT'96*, Lectures Notes in Computer Science 1070, pp. 387-398. Springer-Verlag, 1996.

[8] D. Pointcheval, J. Stern. Security Arguments for Digital Signatures and Blind Signatures. *Journal of Cryptology*, vol. 13, pp. pp. 361-396. Springer-Verlag, 2000.

[9] B. Schneier. *Applied Cryptography Protocols, algorithm, and source code in C (Second Edition)*, John Wiley & Sons, Inc. 1996.

[10] C. Schnorr. Efficient signature generation for smart cards. In: *Advances in Cryptology CRYPTO'89*, Lectures Notes in Computer Science 435. pp. 239-252. Springer-Verlag, 1989.

[11] V. Shoup. Lower Bounds for Discrete Logarithms and Related Problems. In: *Advances in Cryptology EUROCRYPT'97*, Konstanz, Germany, Lectures Notes in Computer Science 1233, pp. 256-266, Springer-Verlag, 1997.

[12] S. Vaudenay. Hidden Collisions on DSS. In: *Advances in Cryptology CRYPTO'96*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 1109, pp. 83-88, Springer-Verlag, 1996.

[13] S. Vaudenay. The Security of DSA and ECDSA– Bypassing the Standard Elliptic Curve Certification Scheme, http://lasecwww.epfl.ch/pub/lasec/doc/Vau03a.ps.

[14] X. Wang, Y. Yin, H. Yu. Finding Collisions in the Full SHA-1. In: *Advances in Cryptology CRYPTO 2005*, Lectures Notes in Computer Science 3621, pp. 17-36. Springer-Verlag, 2005.