On the Length of Hash-values for Digital Signature Schemes

Chae Hoon Lim and Pil Joong Lee
Dept. of Electrical Engineering, Pohang University of Science and Technology,
Pohang, 790-784, KOREA

Abstract

In digital signature schemes derived from the zero-knowledge proof techniques, some authors often claims that the length of hash-values for their schemes could be as short as 64 or 72 bits for the security level of 2^{-64} or 2^{-72}. This letter shows that signature schemes with such short hash values cannot achieve the security levels as stated, due to the birthday attack by the signer.

Keywords : One-way hash functions, Digital signatures, Zero-knowledge proofs.

Introduction: Since the Fiat-Shamir scheme [1], a lot of identification (or authentication) schemes based on the zero-knowledge proof techniques have been developed and all these identification schemes can be converted into digital signature schemes by replacing the verifier's role by pseudo-random functions such as one-way hash functions. Furthermore, most authors of these schemes claimed that t-bit hash values were sufficient to achieve the security level of 2^{-t}, based on the observation that the birthday attack seems not applicable to these schemes. For example, Fiat and Shamir, and Schnorr [2] suggested (at least) $t = 72$, and Guillou and Quisquater [3, 4] even suggested $t = 64$.

In this letter, we show that the length of hash values should be at least 128 for these signature schemes as well. That is, at least $2t$-bit hash values are required to achieve the security level of 2^{-t}. The reason is that the birthday attack is also applicable to these signature schemes when the attacker is the signer himself. Most researchers overlooked the possibility of the signer's denial of his signatures and only considered the attacks by outsiders. We show that for legality of digital signatures the birthday attack should be made infeasible even by the signer. Our result will be illustrated only with the Schnorr signature scheme since it can be applied to other schemes as well.

Schnorr Signature Scheme : Let p and q be two large public primes such that $p \geq 2^{512}$, $q \geq 2^{140}$, and $q|p-1$. Let g be an element of order q in $\mathbf{Z}_p$ and h be a one-way hash function producing t-bit outputs ($t \geq 72$). Denote by (s, v) the secret and public key pair of the signer, where $v = g^{-s} \bmod p$ with $s \in \mathbf{Z}_q$.

Signature Generation. To sign message m, the signer performs the following steps :

0) (Preprocessing) Pick a random number $r \in \mathbf{Z}_q$ and compute $x = g^r \bmod p$.

1) Compute $e = h(x, m) \in \{0, \ldots, 2^t - 1\}$.

2) Compute $y = r + se \bmod q$ and output the signature (e, y).

Signature Verification. To verify the signature (e, y) for message m, the verifier computes $\underline{x} = g^y v^e \mod p$ and checks that $e = h(\underline{x}, m)$.

Birthday Attack by Outsiders : In any one-way hash function h, collison-free or not, giving t-bit outputs, one can find a collision, a pair of distinct inputs m_1 and m_2 such that $h(m_1) = h(m_2)$, in order of $2^{t/2}$ steps using the birthday paradox. For this, one prepares, by a systematic method, two sets of $2^{t/2}$ message variants for each message m_1 and m_2, sorts the hash values of these $2^{t/2+1}$ messages and then searchs for equality. The birthday paradox shows that with a probability $1 - e^{-1}$ one value from the first set equals one value from the second set if the hash function h produces randomly and uniformly a value from $\{0, \ldots, 2^t - 1\}$.

The RSA signature scheme is well-known to be susceptible to the birthday attack. The attacker finds a collision of two messages : one favorable to the signer and the other favorable to himself. When the attacker obtains the signature for the message favorable to the signer, he can reveal the second message favorable to himself. Thus it is recommanded that the bit-length of hash values for RSA should be at least 128.

Unlike the RSA scheme, signature schemes derived from the zero-knowledge proof techniques such as Fiat-Shamir [1], Guillou-Quisquater [3] and Schnorr [2], seem not vulnerable to the birthday attack, as far as the outside attackers are concerned. For example, in the Schnorr scheme, the verification equation can be written as $h(g^y v^e \bmod p, m) = e$. Due to the involvement of hash value e in the argument of the hash function h, it is of little use to find a collision pair of input messages. This is the reason of Schnorr's claim that t-bit hash values can achieve the security level of 2^{-t}. Based on the same argument, Guillou et al. claimed that even a 64-bit hash value is secure for their signature scheme (see [4, page 604]).

Requirements of Digital Signatures : For a digital signature to be accepted as a legal proof, it must have the properity that it could not have been produced by anyone else and can be used by a refree to resolve disputes. The unforgeability is the most crucial property of signatures in either hand-written signatures or digital signatures. However, on digital signatures we must put another requirement for a dispute resolution :

"It must be computationally infeasible even to the signer to find two different messages with the same signature".

Suppose that the signer can find two different messages with the same signature and are forced to sign a message unfavorable to himself. Then he can find a different message favorable to himself with the same signature and later deny the signature for the former message by presenting the latter message. It seems hard for a refree to resolve such a dispute since the signature is valid for either messages. This shows that the above requirement for digital signature schemes is crucial for the guarantee of undeniability by the signer.

Birthday Attack by the Signer : Now we illustrate with the Schnorr signature scheme that it is easy for the signer to find two different messages with the same signature

by the birthday attack, even in the signature schemes derived from the zero-knowledge concept. Suppose that the signer wishes to find two different messages m_1 and m_2 with the same signature (e, y). Then he can proceed as follows, where we assume that $t = 72$, the minimal value of t suggested by Schnorr.

0) (Preprocessing) Pick a random number $r \in \mathbf{Z}_q$ and compute $x = g^r \bmod p$.

1) Prepare two sets of 2^{36} message variants for each message m_1 and m_2, i.e., $M1 = \{m_{1i}\}$ and $M2 = \{m_{2i}\}$ where $i = 1, \ldots, 2^{36}$.

2) Compute two sets of hash values, i.e., $E1 = \{h(x, m_{1i})\}$ and $E2 = \{h(x, m_{2i})\}$ where $i = 1, \ldots, 2^{36}$.

3) Sort the set $E1 \cup E2$ of 2^{37} hash values and search for equality. Assume that the found hash value equal $e = e_{1j} = e_{2k}$ for some j and k.

4) Compute $y = r + se \bmod q$ and output the signature (e, y).

Essentially, finding a collision is as easy in the Schnorr scheme as in the RSA scheme, as far as the attacker is the signer himself. Most authors did not consider the birthday attack by the signer and thus claimed that short hash values such as 64 bits (Guillou-Quisquater) or 72 bits (Fiat-Shamir, Schnorr) would be sufficient for their schemes. Evidently, this is not true, as shown above. It is highly recommanded that the length of hash values in any digital signature schemes should be at least 128.

Conclusion : One important point to keep in mind, when deciding the length of hash values in digital signature schemes, is that one has to consider the birthday attack by the signer himself for legality of digital signatures. As a consequence, the security parameters for all the signature schemes derived from the zero-knowledge concept should be increased almost twice to achieve the stated levels of security. This in turn directly affects the computational efficiency of these signature schemes. Most notably, the Fiat-Shamir scheme or its higher degree versions suffer from severe performance degradation. The situation is better for the Schnorr scheme or its variants. Since, to the authors' opinion, it seems impossible to avoid the birthday attack by the signer, we recommand that at least 128 bit hash values should be used for any signature schemes.

References

[1] A.Fiat and A.Shamir : 'How to prove yourself : Practical solution to identification and signature problems', *Advances in Cryptology-Crypto'86*, Springer-Verlag, 1988, pp.186-194.

[2] C.P.Schnorr : 'Efficient signature generation by smart cards', *Journal of Cryptology*, 1991, 4(3), pp.161-174.

[3] L.C.Guillou and J.J.Quisquater : 'A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory', *Advances in Cryptology-Eurocrypt'88*, Springer-Verlag, 1988, pp.123-128.

[4] L.C.Guillou, M.Ugon and J.J.Quisquater : 'The smart card : A standardized security device dedicated to public cryptology', *Contemporary cryptology - The science of information integrity*, Ed. by G.J.Simmons, IEEE Press, 1992, pp.561-614.