Comments on "Digital signature for Diffie-Hellman public keys without using a one-way function"

Jong-Hyeon Lee

University of Cambridge, Computer Laboratory
Pembroke Street, Cambridge CB2 3QG
jhl21@cl.cam.ac.uk

Abstract. In his recent paper [5], Harn suggested a digital signature scheme using Diffie-Hellman public keys without using one-way functions. It has restriction on the choice of the messages to be signed, and it makes restrictions on the application of the scheme. To become a secure signature, this scheme has to overcome some vulnerability and the native problems of the Diffie-Hellman type protocols; the author reviews some problems in this type.
Indexing terms: public key cryptography, Diffie-Hellman scheme, digital signature.

Introduction: We have seen a number of proposals and attacks on the protocols based on the discrete logarithm problems such as Diffie-Hellman key exchange and ElGamal signature. The protocols based on the discrete logarithm problems are regarded as one of two main stream signature schemes with the factorization-based ones such as the RSA algorithm. The Diffie-Hellman key exchange is a lightweight seminal key exchange scheme [3], however, it cannot be used in signature. In this context, ElGamal signature [4] is regarded as a desired alternative of RSA, but some problems were found and it triggered the development of the Digital Signature Algorithm (DSA) [1].

L Harn has written a series of papers on discrete logarithm-based digital signature schemes. In [7], Harn and Xu classified and generalised the ElGamal type digital signature. In his recent paper [5], he pointed out the danger of using hash functions in ElGamal-like signature schemes, and suggested a digital signature scheme with Diffie-Hellman public keys without one-way functions. Harn claims that all ElGamal signature scheme should sign on the one-way hash of the message, but that hash functions, such as MD4, MD5 or SHA, are at the edge of risking succesful cryptanalytic attack. That is the reason why he wants to sign without one-way functions.

This scheme has some restrictions such that Diffie-Hellman public key is regarded as a message to be signed itself. It reduces the applicability of this scheme. The Diffie-Hellman key updating procedure can be a candidate for the scheme.

This scheme provided four possible signature equations and their verification equations with parameters. However, this scheme also lacks some security considerations as other Diffie-Hellman-type protocols do. It is vulnerable to the middleperson attacks and it is required to carefully choose protocol parameters such as a generator in a finite field, secret random number, and modulus. In the following section, the analysis of Harn's recent scheme and some attacks on this scheme will be described.

Analysis of Harn's scheme: Harn's scheme is built on the assumptions of general Diffie-Hellman key exchange scheme. Let p be a large prime and α be a generator of GF(p). The signer chooses a secret random integer k in $[1, p-2]$ privately such that $r = \alpha^k \pmod p$ becomes the message itself in $[1, p-1]$. Since Diffie-Hellman public key r is a random number, this scheme cannot be applicable for signing on any given message. It is not a complete signature in terms of the functionality.

Let x be a fixed secret key in $[0, p-1]$ and y be a computed fixed public key with $y = \alpha^x \pmod p$. To avoid using a one-way function for making a signature, a linear relation between two secret parameters x and k is adopted. This point makes the scheme a generalisation of Yen and Laih's signature scheme [10] and that of ElGamal signature scheme [4, 6]. Yen and Laih's signature can be a special case of Harn's signature. The signature s for the random public key r satisfies linear equation

$$ax = bk + c \bmod \phi(p), \tag{1}$$

where (a, b, c) are parameters selected from the pair (r, s). Due to the security consideration, c cannot be zero in $\bmod \phi(p)$, and r and s can be replaced with a, b, or c. The equation (1) then becomes a function of public information (r, s) and secret information (x, k). The verification equation for this signature is

$$y^a = r^b \alpha^c \pmod p. \tag{2}$$

In this context, Harn listed four possible pairs of signature-verification equations. In this list, the signature s can be $rx - k$, $x - rk$, $(k + r)/x$, or $(x - r)/k$. When $s = x - rk$, it becomes Yen and Laih's signature except the assumption on the message and Diffie-Hellman public key.

The application of the scheme: Since this scheme is restricted on the choice of messages to be signed, it may not be easy to find its applications. As the Diffie-Hellman public key can be a message itself, we may think of Diffie-Hellman key updating. The whole point of the key updaing is forward security. If the new key is compromised, the old one must not be. However, whether you have the signature equation $s = rx - k$, $s = x - rk$, $s = (k + r)/x$, or $s = (x - r)/k$, the knowledge of new secret key k immediately gives the knowledge of the old secret key x, since (r, s) is public. This scheme cannot be used for Diffie-Hellman key updating.

Attacks on the choice of weak generators: In the way of Beichenbacher's attack [2], this scheme can be forged under the choice of a weak generator. That is, if a weak generator is chosen in this scheme, we can find a valid signature without knowing the secret. The following theorem shows what sorts of the generator choice can be vulnerable.

Theorem 1. *Let $p-1 = bw$, where b is smooth and let y be the public key. If a generator $\beta = cw$ with $0 < c < b$ and an integer t are known such that $\beta^t \equiv \alpha \pmod{p}$, then a valid signature s can be found.*

Proof. Consider a case of above four types: the signature equation $s = rx - k \pmod{\phi(p)}$ and its verification equation $y^r = r\alpha^s \pmod{p}$. The other cases are similarly described to this case.
Since $p-1 = bw$, the subgroup H generated by α^w has order b. Since b is smooth, we can use Pohlig and Hellman's algorithm [9] to compute discrete logarithm in H. So we can find z such that $\alpha^{wz} = y^w \pmod{p}$. Let

$$\begin{aligned} &r = \beta \text{ and} \\ &s = cwz - \frac{1}{t} \pmod{p-1}. \end{aligned}$$

Then

$$\begin{aligned} r\alpha^s &= \beta\beta^{ts} = \beta^{ts+1} = \beta^{cwzt} \\ &= (\beta^t)^{cwz} = \alpha^{cwz} = y^{cw} = y^\beta = y^r. \end{aligned}$$

Hence s is a valid signature. □

Middleperson attack: Consider the traditional middleperson attack. Charlie sits between Alice and Bob. Charlie sets up keys for Alice and Bob. He then relays messages between Alice and Bob, and replaces Alice's message and signature with his message and signature to impersonate Alice to Bob. The Diffie-Hellman key exchange scheme is vulnerable to the middleperson attack. Since Harn's signature scheme is based on Diffie-Hellman scheme and there is no additional protection to this scheme, this scheme inherited the weakness against the middleperson attack.

Conclusion: Harn's digital signature scheme without using hash function is very restricted. We showed that it cannot be applicable for forwarding security such as key exchange. We reminded that this scheme is vulnerable to the middleperson attack.

References

1. RJ Anderson and S Vaudenay, "Minding your p's and q's", *Advances in Cryptology – ASIACRYPT '96*, Kyungju, 1996, pp 26-35.

2. D Bleichenbacher, "Generating ElGamal signatures without knowing the secret key", *Advances in Cryptology – EUROCRYPT '96*, Zaragoza, 1996, pp 10-18.
3. W Diffie and ME Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, **IT-22**(6), 1976, pp 644-654.
4. T ElGamal, "A public key cryptosystem and signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory*, **IT-31**(4), 1985, pp 469-472.
5. L Harn, "Digital signature for Diffie-Hellman public keys without using a one-way function", *Electronic Letters* **33**(2), 1997, pp 125-126.
6. L Harn, "New digital signature scheme based on discrete logarithm", *Electronic Letters* **30**(5), 1994, pp 396-398.
7. L Harn and Y Xu, "Design of generalised ElGamal type digital signature schemes based on discrete logarithm", *Electronic Letters* **30**(24), 1994, pp 2025-2026.
8. K Nyberg, "Comment: New digital signature scheme based on discrete logarithm", *Electronic Letters* **30**(6), 1994, pp 481.
9. SC Pohlig and ME Hellman, "An improved algorithm for computing logarithm over $GF(p)$ and its cryptographic significance", *IEEE Transactions on Information Theory*, **IT-24**(1), 1978, pp 106-110.
10. S-M Yen and C-S Laih, "New digital signature scheme based on discrete logarithm", *Electronic Letters* **29**(12), 1993, pp 1120-1121.