Published in *Electronics Letters*, **Vol. 34, No. 18, pp. 1738–1739, September 1998.**

Improved authenticated multiple-key agreement protocol

Sung-Ming Yen and Marc Joye

Indexing terms: Cryptography, Data integrity, Key agreement protocol, Diffie-Hellman scheme, Digital signature

Recently, Harn and Lin (1998) developed a two-phase authenticated key agreement protocol which enables two parties to share multiple secret keys. The first phase of their protocol is the most important part and can be used to deliver a sequence of temporary random public keys to the other party in an authenticated approach. The authors demonstrate an improved version of this novel scheme after giving some cryptanalytic details of the original Harn-Lin scheme.

Authenticated key agreement protocol: In [1], Harn and Lin developed a two-phase authenticated key agreement protocol which enables two parties to share multiple secret keys. In the first phase of their protocol, n temporary random public keys are delivered to the other party in an authenticated approach. A Diffie-Hellman [2]-like key distribution method is employed in the second phase by the two communication parties to share n^2-1 independent secret keys.

In the following, for the purpose of demonstrating a possible weakness if the system is not carefully designed and to show how to develop possible modifications, a special example of the protocol will be reviewed. There are two parties A and B involved in the protocol; however, only the role played by A will be described, B acting in a similar manner. Party A randomly selects two short-term secret numbers k_{A1} and k_{A2} and computes their corresponding public counterparts (we call them the temporary random public keys) $r_{A1} = \alpha^{k_{A1}} \bmod P$ and $r_{A2} = \alpha^{k_{A2}} \bmod P$ where P is a prime number and α is a primitive element in $\mathbb{F}_P^*$. Two mixed parameters are then evaluated as $k_A = (k_{A1} + k_{A2}) \bmod (P-1)$ and $r_A = \alpha^{r_{A1} \cdot r_{A2}} \bmod P$. Party A then uses one of the signature schemes reported in [3] for certifying the two public numbers r_{A1} and r_{A2} as

$$s_A = (x_A - r_A \cdot k_A) \bmod (P-1) \tag{1}$$

where x_A is the party A's personal/long-term secret key and s_A is the number to be evaluated. Finally, party A sends

$$\{r_{A1}, r_{A2}, s_A, cert(y_A)\}$$

to party B where $cert(y_A)$ is the certification of public key $y_A = \alpha^{x_A} \bmod P$. Of course, party B does similar computations and sends $\{r_{B1}, r_{B2}, s_B, cert(y_B)\}$ to A.

For party B, the most important parts of the above protocol are the authenticity and the data integrity check of the received r_{A1} and r_{A2}. Party B uses the same method to compute r_A, i.e., $r_A = \alpha^{r_{A1} \cdot r_{A2}} \bmod P$. Via the following computation

$$y_A \stackrel{?}{\equiv} (r_{A1} \cdot r_{A2})^{r_A} \cdot \alpha^{s_A} \pmod P, \tag{2}$$

party B can be convinced of the authenticity and the integrity of both r_{A1} and r_{A2} as announced in [1].

In the second phase of the protocol, a multiple-key distribution/generation process is performed. Suppose that A has already received $\{r_{B1}, r_{B2}, s_B, cert(y_B)\}$ and has verified the authenticity and the integrity of r_{B1} and r_{B2}. Party A then derives $K_1 = r_{B1}^{k_{A1}} \bmod P$, $K_2 = r_{B1}^{k_{A2}} \bmod P$, $K_3 = r_{B2}^{k_{A1}} \bmod P$, and $K_4 = r_{B2}^{k_{A2}} \bmod P$. Only 3 of the 4 keys will be used in order to provide *perfect forward secrecy* [4], which means that an adversary cannot deduce all of the shared common secret keys between A and B if one of the keys has been learned. The topic is impor-

Cryptanalysis of Harn-Lin scheme: One straightforward modification of the above protocol is to let

$$r_A = \alpha^{k_{A1} + k_{A2}} \bmod P.$$

However, it will be shown that this modified key agreement protocol provides no authentication of integrity for both r_{A1} and r_{A2}. Here, we assume that all the other parts of the protocol remain identical and the equation used to compute s_A now becomes

$$\begin{aligned} s_A &= (x_A - r_A \cdot k_A) \bmod (P-1) \\ &= (x_A - [r_{A1} \cdot r_{A2} \bmod P] \cdot k_A) \bmod (P-1). \end{aligned} \tag{3}$$

The cheater can arbitrarily select r'_{A1} and r'_{A2} such that

$$r_A \equiv r'_{A1} \cdot r'_{A2} \equiv r_{A1} \cdot r_{A2} \pmod P$$

and pass

$$\{r'_{A1}, r'_{A2}, s_A, cert(y_A)\}$$

to party B. Evidently, party B will also be convinced of the integrity of both r'_{A1} and r'_{A2} via the same previously mentioned checking equation, i.e., Eq. (2). Owing to the lack of cryptanalysis of the original protocol reported in [1], it is not clear why r_A was chosen to be $r_A = \alpha^{r_{A1} \cdot r_{A2}} \bmod P$. It is supposed that the main reason is to make the protocol free from the above demonstrated attack.

It can be shown that for the above attack to work in the original protocol proposed by Harn and Lin, the following conditions should be satisfied:

$$\begin{cases} r'_{A1} \cdot r'_{A2} \equiv r_{A1} \cdot r_{A2} \pmod P, \\ r'_{A1} \cdot r'_{A2} \equiv r_{A1} \cdot r_{A2} \pmod{(P-1)} \end{cases} \tag{4}$$

$$\iff r'_{A1} \cdot r'_{A2} \equiv r_{A1} \cdot r_{A2} \pmod{\operatorname{lcm}(P, P-1)}.$$

But since $\operatorname{lcm}(P, P-1) = P(P-1) > (P-1)^2$ and since r_{A1}, r_{A2}, r'_{A1}, and $r'_{A2} \in \mathbb{F}_P^*$ (and thus $\leq (P-1)$), we have

$$r'_{A1} \cdot r'_{A2} = r_{A1} \cdot r_{A2}, \tag{5}$$

over the reals. Therefore, given r_{A1} and r_{A2}, let q be a small factor of r_{A1}, then we take $r'_{A1} = r_{A1}/q$ and $r'_{A2} = r_{A2} \cdot q$. Note that r_{A1} is divisible by a small factor with high probability; moreover $r'_{A2} = r_{A2} \cdot q$ will be smaller than P with some probability. Note also that we can try simultaneously with a small factor of r_{A2}. This implies that the original Harn-Lin scheme is not secure. The following example clarifies the claim.

Example 1. Let $r_{A1} = 2$, $r_{A2} = 9$, and $P = 17$, then the cheater can forge $r'_{A1} = 6$ and $r'_{A2} = 3$.

Fortunately, the previous forgery can be prevented by imposing both r_{A1} and r_{A2} to be in the range $[\lceil P/2 \rceil, P-1]$. Since 2 is the smallest possible factor of either r_{A1} or r_{A2}, then either $2 \cdot r_{A1}$ or $2 \cdot r_{A2}$ will be greater than P. It is therefore impossible for the cheater to find such r'_{A1} and r'_{A2} under this modification.

Improved protocol: A more simple and efficient alternative can be developed which can also be free from the above demonstrated attack; of course, both r_{A1} and r_{A2} should be in the range $[\lceil P/2 \rceil, P-1]$. In this improved protocol, party A computes $k_A = (k_{A1} + k_{A2}) \bmod (P-1)$ as before but the parameter r_A is not needed now and this eliminates one expensive *modular exponentiation* computation. The signature generation equation Eq. (1) to certify both r_{A1} and r_{A2} is replaced by

$$s_A = (x_A - (r_{A1} \cdot r_{A2}) \cdot k_A) \bmod (P-1) \tag{6}$$

and the authenticity and integrity checking equation becomes

$$y_A \stackrel{?}{\equiv} (r_{A1} \cdot r_{A2})^{(r_{A1} \cdot r_{A2})} \cdot \alpha^{s_A} \pmod P. \tag{7}$$

faces the situation of solving the impossible problem in Eq. (4) of finding a pair (r'_{A1}, r'_{A2}) different from (r_{A1}, r_{A2}).

It is extremely important to notice the main difference between this improved protocol and the previously mentioned insecure modification. This can be summarized in terms of the signature generation equation as

Improved protocol: $x_A \equiv (r_{A1} \cdot r_{A2}) \cdot k_A + s_A \pmod{P-1}$
Insecure modification: $x_A \equiv [r_{A1} \cdot r_{A2} \bmod P] \cdot k_A + s_A \pmod{P-1}$.

Finally, note that for party B, since the parameter r_A is not required, one expensive *modular exponentiation* computation can also be eliminated, as for party A.

Acknowledgement: This work was supported by the National Science Council of the Republic of China under contracts NSC87-2213-E-032-012 and NSC87-2811-E-032-0001.

26 June 1998

Sung-Ming Yen and Marc Joye (*LCIS, Dept of Electrical Engineering, Tamkang University, Tamsui, Taipei Hsien, Taiwan 25137, Republic of China*)

E-mail: {yensm,joye}@ug.ee.tku.edu.tw

References

1 L. Harn and H.Y. Lin, 'An Authenticated Key Agreement Protocol Without Using One-way Functions', *Proc. of 8th National Conf. on Information Security*, Kaoshiung Taiwan, (May 1998), pp.155–160.

2 W. Diffie and M.E. Hellman, 'New Directions in Cryptography', *IEEE Trans. on Inform. Theory*, **IT-22** (6), (Nov. 1976), pp.644-654.

3 L. Harn, 'Digital Signatures for Diffie-Hellman Public Keys Without Using A One-way Function', *Electronics Letters*, **33** (2), (Jan. 1997), pp.125–126.

4 C.H. Lim and P.J. Lee, 'Security of Interactive DSA Batch Verification', *Electronics Letters*, **30** (19), (Sep. 1994), pp.1592–1593.