Pre-proceedings of

EUROCRYPT '94

May 9-12, 1994
University of Perugia, Italy

A workshop on the Theory and Applications
of Cryptographic Techniques

Sponsored by
the International Association for Cryptologic Research (IACR)

Organized by
Istituto Internazionale delle Comunicazioni (IIC)
Fondazione Ugo Bordoni (FUB)

In cooperation with
Amtec
Italcable
Scuola Superiore Gugliemo Reiss Romoli (SSGRR)
Telsy Elettronica Telecomunicazioni
University of Perugia
A Secure and Efficient Conference Key Distribution System

(Extended Abstract)

Mike Burmester*
Department of Mathematics
Royal Holloway - University of London
Egham, Surrey TW20 OEX
U.K.

Yvo Desmedt
Department of EE & CS
University of Wisconsin - Milwaukee
P.O. Box 784, WI 53201 Milwaukee
U.S.A.

Abstract

We present a practical interactive conference key distribution system based on public keys, which is 'proven' secure provided the Diffie-Hellman problem is intractable. The system authenticates the users and allows them to compute their own conference key. A certain number of interactions is required, but the number of rounds is independent of the number of conference users. All users involved perform the same amount of computation and communication. Our technique for authentication can be extended and used as the basis for an authentication scheme which is 'proven' secure against any type of attack, provided the discrete logarithm problem is intractable.

•Research partly carried out while visiting the University of Wisconsin - Milwaukee.
A Secure and Efficient Conference Key Distribution System

(Extended Abstract)

Abstract

We present a practical interactive conference key distribution system based on public keys, which is 'proven' secure provided the Diffie-Hellman problem is intractable. The system authenticates the users and allows them to compute their own conference key. A certain number of interactions is required, but the number of rounds is independent of the number of conference users. All users involved perform the same amount of computation and communication. Our technique for authentication can be extended and used as the basis for an authentication scheme which is 'proven' secure against any type of attack, provided the discrete logarithm problem is intractable.

1 Introduction

To communicate securely over insecure channels it is essential that secret keys are distributed securely. Even if the encryption algorithm used is computationally infeasible to break, the entire system is vulnerable if the keys are not securely distributed. Key distribution is central to cryptography and has attracted a lot of attention (e.g., [18, 26, 8, 32, 28, 33]). Research has focused on security and on efficiency. Many practical systems have been proposed [32, 28, 33, 39, 19, 41]. The most familiar system is the Diffie-Hellman key distribution system [18]. This enables two users to compute a common key from a secret key and publicly exchanged information. However it does not authenticate the users, except for the public key version, in which case the session key is fixed.

If more than two users want to compute a common key, then a conference key distribution system is used. Designing such systems can be particularly challenging because of the complexity of the interactions between the many users- Many conference key distribution systems have been presented recently [26, 27, 33, 39, 21, 10]. These however are either impractical, or only heuristic arguments are used to address their security. Our goal in this paper is to present a practical and proven secure conference key distribution system.

Ingemarsson, Tang and Wong proposed a conference key distribution system for which the common key is a symmetric function [26]. This has many attractive features but is insecure because the information exchanged by the users makes it possible for a passive eavesdropper to compute the key. Our system is similar but uses a cyclic function. This prevents the attack by passive eavesdroppers whilst retaining the efficiency of the former scheme. The number of rounds (exchanges) which are required to compute the common key is independent of the number of conference users. For authentication we use a public key (interactive) authentication scheme which is proven secure against any known (generic chosen [24]) text attack, if the Discrete Logarithm problem is intractable. Combining the two systems we get a conference
key distribution scheme which is provably secure against any type of attack, including those by malicious active adversaries working together, provided the Diffie-Hellman problem is intractable.

Our authentication scheme is of interest in itself, because of its efficiency and proven security. We note that all proven secure signature schemes presented so far [24, 30, 36, 2, 3] are impractical. We therefore extend our scheme so that it is proven secure against any type of attack, including adaptive chosen text attacks by real-time middle-persons, under the same cryptographic assumption. The resulting scheme is roughly as fast as RSA [35], but in addition is proven secure.

The organization of this paper is as follows. In Section 2 we give definitions and present our model for conference key distribution systems and for authentication schemes. In Section 3 we present a protocol for a conference key distribution system which is secure against attacks by passive eavesdroppers provided the Diffie-Hellman problem is hard. In Section 4 we present an authentication scheme and in Section 5 we combine the two to get a conference key distribution scheme which is secure against any type of attack. In Section 6 we extend the security of our authentication scheme, and we conclude in Section 7.

2 Definitions

We consider networks in which the users can broadcast 'messages' (strings) to each other. We allow for the possibility that an eavesdropper (a malicious adversary) may read the broadcast messages or substitute some of them. We distinguish two types of networks: those for which is passive and those for which is active. Let \( N \) be the security parameter.

Definition 1. Suppose that \( n = O(N^c), c > 0 \) constant, interactive Turing machines \( U_1, \ldots, U_n \) take part in a protocol to generate a key. We say that the protocol is a conference key distribution system if, when all the \( U_1, \ldots, U_n \) are as specified, then each \( U_i \) computes the same key \( K = K_i \). A conference key distribution system guarantees privacy if it is computationally infeasible for a passive eavesdropper to compute the key \( K \).

Definition 2. Suppose that \( n = O(N^c) \) interactive Turing machines \( U_1, \ldots, U_n \) use a conference key distribution system, and that each \( U_i \) has received (from an oracle) a secret key \( S_i \) (written on its knowledge

---

2 A network is a collection of \( n \) interactive probabilistic Turing machines \( U_i \) with \( n - 1 \) write-only tapes, \( n - 1 \) read-only tapes, a history tape, a knowledge tape and worktapes.

3 An eavesdropper is an interactive probabilistic Turing machine with \( n(n - 1) \) read-only tapes \( T_{ij} \) and \( n(n - 1) \) write-only tapes \( W_{ij} \). The eavesdropper reads from \( T_{ij} \) and writes on \( W_{ij} \). If what is written is different from what is read then the eavesdropper is active. Otherwise the eavesdropper is passive. This, together with our definition of a network, allows for a scenario in which a broadcasted message can be substituted for each individual receiver. Eavesdroppers are polynomially bounded.
tape) which corresponds to its public key \( k_i \), which is published. Let \( n' > 0 \) of these be honest, \( n'' = n - n' \geq 0 \) be impersonators, and assume that there is a secure network between the impersonators and the (passive or active) eavesdropper. We say that a conference key distribution system is (computationally) secure, if it is computationally infeasible for any set of \( n'' \), \( 0 \leq n'' < n \), impersonators \( U_j' \) in collaboration with the eavesdropper to compute the same key \( K_i \) as computed by any of the honest machines \( U_i \).

Remark 1. If the set of impersonators is empty we require that the (active) eavesdropper cannot compute \( K_i \).

Definition 3. (Informal) Consider a network with eavesdropper \( E \). A protocol \((U_1, U_2)\) in which \( U_1 \) sends a message \( m \) is an authentication system if,

- **Compliance**: When \( U_1, U_2 \) are honest and \( E \) is passive then \( U_2 \) accepts and outputs \( m \) with overwhelming probability,
- **Secure against impersonation**: \( U_2 \) rejects with overwhelming probability a dishonest \( U'_j \),
- **Secure against substitution**: If \( E \) is active and \( U_2 \) outputs \( m' \neq m \) then \( U_2 \) rejects with overwhelming probability.

Definition 4. The Diffie-Hellman [18] problem: given \( p, a, \beta, \gamma \), find \( \beta^{\log_\gamma a} \mod p \) if it exists.

Breaking this problem has remained an open problem for more than 15 years. Even if the factorization of the order of \( \alpha \) is known the problem is assumed to be hard (cf. [9, 11, 12]). It is well known [31, 16, 29, 25] that if the Discrete Logarithm problem is easy then so is the Diffie-Hellman problem, but the converse may not be true.

3 A conference key distribution system

A center chooses a prime \( p = \Theta(2^{cN}) \), \( c \geq 1 \) constant, and an element \( \alpha \in \mathbb{Z}_p \) of order \( q = \Theta(2^N) \). If this has to be verified then the factorization of \( q \) is given. The center publishes \( p, \alpha \) and \( q \).

Protocol 1. Let \( U_1, \ldots, U_n \) be a (dynamic) subset of all users who want to generate a common conference key.

---

4 An honest machine \( U_i \) has a secret key \( s_i \) written on its knowledge tape. An impersonator \( U_j' \) is any polynomially bounded interactive probabilistic Turing machine which replaces \( U_j \) but does not have the secret key of \( U_j \) (or an equivalent). In our model the eavesdropper is not an impersonator: it can only impersonate \( U_j \) with the help of an impersonator (if there is one). We will strengthen the definition in the final paper.

5 An abuse of notation: there may be more than \( n \) users altogether.
Step 1. Each $U_i, i = 1, \ldots, n$, selects $r_i \in R Z_q$, computes and broadcasts $z_i = \alpha^{r_i} \mod p$.

Step 2. Each $U_i, i = 1, \ldots, n$, checks that $\alpha^q \equiv 1 \mod p$ and that $(z_j)^q \equiv 1 \mod p$ for all $j = 1, \ldots, n$, and then computes and broadcasts

$$X_i \equiv (z_{i+1}/z_{i-1})^{r_i} \mod p,$$

where the indices are taken in a cycle.

Step 3. Each $U_i, i = 1, \ldots, n$, computes the conference key,

$$K_i \equiv (z_{i-1})^{r_i} \cdot X_i^{q-1} \cdot X_i^{q-2} \cdot X_{i+1} \cdot \ldots \mod p.$$ 

Remark 2. Honest users compute the same key,

$$K \equiv \alpha^{r_1 + r_2 + \ldots + r_n} \mod p.$$ 

Indeed, set $A_{i-1} \equiv (z_{i-1})^{r_i} \equiv \alpha^{r_i} \mod p$, $A_i \equiv (z_{i-1})^{r_i} \cdot X_i \equiv \alpha^{r_i + 1} (\mod p)$, $A_{i+1} \equiv (z_{i-1})^{r_i+1} \cdot X_i \cdot X_{i+1} \equiv \alpha^{r_i+1} \mod p$ etc., and we have $K_i = A_{i-1} \cdot A_i \cdot A_{i+1} \cdot \ldots \mod p$. So the key is a second order cyclic function of the $r_i$ (but not symmetric as in [26]).

For $n = 2$ we get $X_1 = X_2 = 1$ and $K \equiv \alpha^{r_1 + r_2} \equiv \alpha^{2r_1} \mod p$, which is essentially the same as for the Diffie-Hellman [18] system (clearly there is no need to broadcast $X_1, X_2$ in this case).

Theorem 1. If $n$ is even and polynomially bounded in the length of $p$, and if the Diffie-Hellman problem is intractable, then Protocol 1 is a conference key distribution system which guarantees privacy.

Proof. From Remark 2 it follows that Protocol 1 is a conference key distribution system. We prove that it guarantees privacy by contradiction. Suppose that a passive eavesdropper $E$ succeeds with non-negligible probability in breaking the key $K_1 = (z_n)^{r_1} \cdot X_1^{q-1} \cdot X_2^{q-2} \cdot \ldots \cdot X_{n-1} \mod p$ of $U_1$. We shall show how to use the program of $E$ to break the Diffie-Hellman problem for any instance $z_n, z_1$.

We prepare the rest of the input to be given to $E$. Select numbers $b_2, b_3, \ldots, b_{n-1}$ at random from $Z_q$, and compute:

$$z_2 \equiv z_n \cdot \alpha^{b_2} \mod p, \quad z_3 \equiv z_1 \cdot \alpha^{b_3} \mod p, \quad \ldots, \quad z_{n-1} \equiv z_{n-3} \cdot \alpha^{b_{n-1}} \mod p. \quad (1)$$

Since $n$ is even we must also have,

$$z_n \equiv z_2 \cdot \alpha^{-b_2} \equiv z_4 \cdot \alpha^{-b_4} \equiv \ldots \equiv z_{n-2} \cdot \alpha^{-b_{n-2}} \mod p,$$

$$z_1 \equiv z_3 \cdot \alpha^{-b_3} \equiv z_5 \cdot \alpha^{-b_5} \equiv \ldots \equiv z_{n-1} \cdot \alpha^{-b_{n-1}} \mod p. \quad (2)$$

6 We use the notation $a \in \mathbb{Z}_p^*$ to indicate that $a$ is selected from the set $A$ uniformly and independently.

7 If the center is trusted (oracle) the first test is not required.
From (1) it follows that \( X_1 \equiv (z_2/z_n)^{r_1} \equiv (\alpha^{r_1})^{b_2} \equiv (z_1)^{b_2} \pmod{p} \), so \( X_1 \) is easy to compute. Similarly for \( X_2, X_3, \ldots, X_{n-2} \). Using (2), \( X_{n-1} \equiv (z_n/z_{n-2})^{r_{n-1}} \equiv (z_{n-1})^{-b_2-b_4-\cdots-b_{n-2}} \pmod{p} \), and \( X_n \equiv (z_1/z_{n-1})^{r_n} \equiv (z_n)^{-b_2-b_4-\cdots-b_{n-1}} \pmod{p} \). So it is feasible to compute all the \( X_i \).

We now have the necessary input for \( E \). That is, the Diffie-Hellman instance \( z_1, z_n \), the computed \( z_2, \ldots, z_{n-1} \) and the computed \( X_1, \ldots, X_n \). From our assumption, \( E \) will obtain the corresponding \( K_1 \). Clearly \( E \) can easily compute \( (z_n)^{r_1} \pmod{p} \) from \( K_1 \). It is well known [7, 34] that it is feasible to compute \( n \)-th residues in \( \mathbb{Z}_p \) when \( n \) is polynomially bounded. \( E \) may not be able to find which one corresponds to \( (z_n)^{r_1} \pmod{p} \), if there are many, so it picks one at random. With non-negligible probability bounded by \( 1/n \) it will pick the right one. Consequently, with non-negligible probability \( E \) can succeed in getting \( (z_n)^{r_1} \pmod{p} \). So we have a violation of the intractability of the Diffie-Hellman problem.

Corollary 1. Theorem 1 can easily be extended to allow for an odd number of users by slightly modifying Protocol 1.

Proof. When the number of users is odd then one user, say the last one, behaves virtually as two independent machines.

Remark 3. Clearly anybody can masquerade as \( U_i \) in Protocol 1. So the users are not authenticated. In the following section we present an authentication scheme which, when combined with this system, offers both privacy and authentication.

Remark 4. The following alternative scheme has been suggested to us. A chair, say \( U_1 \), will distribute the common key. First \( U_1 \) establishes secret keys \( K_{1i} \) with each user \( U_i \) separately (e.g. using the Diffie-Hellman key exchange [18]), and then \( U_1 \) selects a random key \( K \) which it sends to each \( U_i \) encrypted under \( K_{1i} \) (e.g. \( K \oplus K_{1i} \), where \( \oplus \) is bitwise exclusive-or). This solution has a major disadvantage: the chair has to perform \( n-1 \) more computations than the other users. Moreover if broadcasting is as expensive as sending to a single individual (as is the case on ethernet based local area networks), the communication cost of the chair is \( n-1 \) times more than the other users. Our scenario is symmetric in this respect.

4 An authentication scheme

As in Section 3, a center chooses \( p, \alpha \) and \( q \), but now \( q \) is a prime. Then each user \( P \) selects \( a, b \in_R \mathbb{Z}_q \), computes \( \beta = \alpha^a \pmod{p} \), \( \gamma = \alpha^b \pmod{p} \), and registers \( k = (\beta, \gamma) \) as its public key.\(^8\)

\(^8\)There is no need for \( p, q \) to be standard.
Protocol 2. Common input: \((p, \alpha, q, \beta, \gamma)\).

\(P\) has \(a, b\) written on the knowledge tape, where \(\beta = \alpha^a \mod p, \gamma = \alpha^b \mod p\). \(P\) is given \(z \in \mathbb{Z}_q\).

\(P\) authenticates \(z\) to \(V\): \(P\) sends \(z\) to \(V\) and then proves to \(V\) that it knows the discrete logarithm of \(\beta^z \gamma \mod p\) (= \(az + b \mod q\)), by using any interactive zero-knowledge proof of knowledge (e.g., [15, 14, 4, 17]).

\(V\) verifies this and checks that \(\alpha \neq 1 \mod p\), \(\alpha^z \equiv \beta^z \equiv \gamma^z \equiv 1 \mod p\) and that \(q\) is a prime. If this fails \(V\) halts.

Theorem 2. Protocol 2 is an authentication scheme secure against a generic chosen text attack (\(z \in \mathbb{Z}_q\) is chosen independently of \(\gamma\)) if the order of \(\alpha\) is prime, provided the Discrete Logarithm problem is intractable.

Proof. (Sketch) First consider an impersonation attack by \(P'\), which after having observed the history \(h\) of earlier proofs, is accepted by the verifier with non-negligible probability. From the definition of soundness for proofs of knowledge [20, 1] it follows that \(P'\) must know \(az + b \mod q\). \(P'\) is now used as a black box to break the Discrete Logarithm of \(\gamma\). Take as common input \((p, \alpha, q, \alpha^z, \gamma)\), where \(r \in \mathbb{Z}_q\). The history \(h\) can easily be simulated. Then give the common input and \(h\) to \(P'\) to get: \(z \in \mathbb{Z}_q\) and \(r z + DL(\gamma) \mod q\). Since \(z, r\) are known it is easy to compute \(DL(\gamma)\).

Next consider a substitution attack by \(P'\) who succeeds with non-negligible probability in modifying in real time the proof \((P, P')\) of knowledge of \(az + b \mod q\) to a proof \((P', P', V)\) of knowledge of \(az' + b \mod q\), \(z' \neq z\) (after having observed earlier proofs). We shall show that \(PP'\) can be used to break the Discrete Logarithm problem of \(\beta\). Assume that \(P\) has \(az + b \mod q\) on its knowledge tape (only, not \(a, b\)). As in the previous case, \(PP'\) must know \(az' + b \mod q\). Choose \(r \in \mathbb{Z}_q\) (r replaces \(az + b\), \(z \in \mathbb{Z}_q\), and history \(h\), and let \(\gamma \equiv \alpha^r \beta^{-z} \mod p\). So \(z\) must be independently of \(\gamma\) (otherwise we could not take \(r\) to be random). Then input to \(PP'\): \((p, \alpha, q, \beta, \gamma), z, h, r\) on the knowledge tape of \(P',\) to get: \(z'\) and \(DL(\beta) z' + DL(\gamma) \equiv DL(\beta)(z' - z) + r \mod q\). Since \(z', z, r\) are known, it is easy to compute \(DL(\beta)\) when \(z' \neq z\).

Remark 5. Although zero-knowledge proofs do not guarantee inherently secure identification [5], in the context of authentication only real-time attacks in which the message is not authentic (e.g., substituted) make sense. We have discussed such real-time attacks in the proof.

---

\(^9\)These earlier proofs are proofs \((P, V)\) of knowledge of \(az + b\), and proofs \((P, P', V)\) in which \((P, P')\) have used \((k, z)\) and \((P', V)\) have used \((k, z')\).

\(^{10}\)Important technical remarks about proofs of knowledge were discussed in [1]. In the final paper we discuss these issues in our context.
5 An authenticated conference key

Theorem 3. Let $p_1$, $\alpha_1$ and $q_1$ be as in Section 3, and $p_2$, $\alpha_2$ and $q_2$ be as in Section 4 with $q_2$ a prime and $p_1 \leq q_2$. If each $U_i$ authenticates $z_i$ to $U_{i+1}$ as in Protocol 2 with parameters $p_2, \alpha_2, q_2$ and public key $k_i = (\beta_2, \gamma_2)$, before Step 9 of Protocol 1, then the conference key distribution system is secure provided the Diffie-Hellman problem is intractable.

Proof. (Sketch) By permuting the indices the proof is reduced, as in Theorem 1, to showing that successful adversaries can compute $(z_n)^{\gamma_1} \mod p$. Since $z_n$ has been authenticated by $U_n$, the adversaries have no control over it, without $U_1$ finding out. (Clearly the Discrete Logarithm problem is intractable when the Diffie-Hellman problem is intractable.) So the adversaries must succeed in computing $(z_n)^{\gamma_1} \mod p$, knowing only $z_1 = \alpha_1 \mod p$ and $z_n$. As in Theorem 1 this leads to a violation of the intractability of the Diffie-Hellman problem. \[\square\]

Corollary 2. Protocol 2 can be replaced by any proven secure authentication scheme, provided its security assumption is added to the conditions of Theorem 3.

6 A proven secure authentication scheme

The authentication Protocol 2 has not been proven secure against a chosen attack. Indeed in Theorem 2 the proof of security against a substitution attack relies on the independence of the message from $\gamma$ of the public key. We now will modify Protocol 2 to obtain security against all known attacks, including adaptive chosen text attacks.

Let $(p_2, \alpha_2, q_2), (p_3, \alpha_3, q_3)$ be as in Section 4 with $p_2 \leq q_3$, and $k = (\beta_2, \beta_3, \gamma_3)$ be the public key of user $U$, with $\beta_2 = \alpha_2^{b_2} \mod p_2$, $\beta_3 = \alpha_3^{a_3} \mod p_3$, $\gamma_3 = \alpha_3^{b_3} \mod p_3$, $a_2 \in_R Z_{q_2}$, $a_3, b_3 \in_R Z_{q_3}$. The following protocol is used to authenticate any number $z \in Z_{q_2}$:

Protocol 3. Common input: $(p_2, \alpha_2, p_3, \alpha_3, q_3; \beta_2, \beta_3, \gamma_3)$.

$P$ has written on its knowledge tape $a_2, a_3, b_3$, where $\beta_2 = \alpha_2^{a_2} \mod p_2$, $\beta_3 = \alpha_3^{a_3} \mod p_3$, $\gamma_3 = \alpha_3^{b_3} \mod p_3$. $P$ is given $z \in Z_{q_2}$.

$P$ authenticates $z$ to $V$: $P$ sends to $V$: $z$ and $\gamma_2 = \alpha_2^{b_2} \mod p_2$, where $b_2 \in_R Z_{q_2}$, and then proves to $V$, simultaneously, that it knows the discrete logarithm base $\alpha_2$ of $\beta_2^z \cdot \gamma_2 \mod p_2$, where $z \in_R Z_{q_2}$, and the discrete logarithm base $\alpha_3$ of $\beta_3 \cdot \gamma_3 \mod p_3$, by using a zero-knowledge proof of knowledge (e.g., [15, 14, 4, 17]).

$V$ verifies this, checks that $\gamma_2 \equiv 1 \mod p_2$, and then checks that $\alpha \not\equiv 1 \mod p_2$, $\alpha_2^{a_2} \equiv \beta_2^{\gamma_2} \equiv 1 \mod p_2$, $\alpha_3^{a_3} \equiv \beta_3^{a_3} \equiv \gamma_3^{a_3} \equiv 1 \mod p_3$ and that $q_2, q_3$ are primes and $p_2 \leq q_3$. If this fails $V$ halts.
Theorem 4. Protocol 3 is a secure authentication scheme if the Discrete Logarithm problem is intractable.

Proof. (Sketch) The proof is an extension of Theorem 2. The argument for impersonation attacks is essentially the same, so we only consider substitution attacks. Suppose that $P'$ succeeds with non-negligible probability in modifying the proof $(P, P')$ of knowledge of $A_2 \equiv a_2 z + b_2 \pmod{p_2}$ and $A_3 \equiv a_3 z_2 + b_3 \pmod{q_2}$ ($z$ is chosen by $P'$), to a proof $(P, P', V)$ of knowledge of $a_2 z' + b_2 \pmod{q_2}$ and $a_3 z'_2 + b_3 \pmod{q_3}$, with $z' \neq z$, after having observed earlier proofs. Then $PP'$ must know both $a_2 z' + b_2 \pmod{q_2}$ and $a_3 z'_2 + b_3 \pmod{q_3}$, where $z'_2 = a_2^k \pmod{p_3}$. We shall use $PP'$ to break the Discrete Logarithm problem. We distinguish two cases, which we run each with probability one half.

Case 1: $z'_2 \equiv z_2 \pmod{p_3}$. Take $\delta_2 \in_R (a_2)$ ($\delta_2$ replaces $\beta_2$) as an instance for the Discrete Logarithm problem and choose $a_3, b_3 \in_R Z_{q_3}$, and compute $\gamma_3 = \alpha_3^k \pmod{p_3}$. For any given $z \in Z_{q_3}$, take $r_2 \in_R Z_{q_3}$ ($r_2$ replaces $a_2 z + b_2 \pmod{q_2}$), and compute $\gamma_2 = \alpha_2^{r_2} \delta_2^{-z} \pmod{p_2}$ and $r_3 = a_3 z_2 + b_3 \pmod{q_3}$, and a simulated history $h$. Then input to $PP'$: $(\delta_2, \delta_3, \gamma_3, z, h, r_2, r_3)$ on the knowledge tape of $P$, to get: $z'$ and $\gamma'_2, A'_2, A'_3$. If $\gamma'_2 \equiv \gamma_2 \pmod{p_2}$ then $A'_2 \equiv DL(\delta_2)z' + DL(\gamma_2) \equiv DL(\delta_2)(z' - z) + r_2 \pmod{p_2}$, and since $z' \neq z$ we get $DL(\delta_3)$. Else ignore.

Case 2: $z'_2 \neq z_2 \pmod{p_3}$. Take $\delta_3 \in_R (a_3)$ ($\delta_3$ replaces $\beta_3$) as an instance for the Discrete Logarithm problem, and $r_3 \in_R Z_{q_3}$ ($r_3$ replaces $a_3 z + b_3 \pmod{q_3}$) and choose $a_2, b_2 \in_R Z_{q_2}$, and compute $\gamma_2 = \alpha_2^{r_2} \pmod{p_2}$, $\gamma_3 = \alpha_3^{r_3} \delta_3^{-z_2} \pmod{p_2}$. Input to $P$: $(\delta_2, \delta_3, \gamma_3)$, which chooses $z \in Z_{q_2}$. Compute $r_2 = a_2 z + b_2 \pmod{q_2}$, and history $h$. Then input to $PP'$: $(\delta_2, \delta_3, \gamma_3, z, h, r_2, r_3)$ on the knowledge tape of $P$, to get: $z'$, $\gamma'_2, A'_2, A'_3$. If $\gamma'_2 \neq \gamma_2 \pmod{p_2}$ then $A'_2 \equiv DL(\delta_2)\gamma'_2 + DL(\gamma_3) \equiv DL(\delta_2) (\gamma'_2 - \gamma_2) + r_2 \pmod{q_3}$, and we get $DL(\delta_3)$. Else ignore.

7 Conclusion

We have presented a conference key distribution system and proven that it is secure against a passive adversary if the Diffie-Hellman problem (a 15 year open problem) is hard. The session key is a cyclic function (of the indices of the users) of degree two, which is the main reason for its practicality. Ingemarson Tang and Wong considered conference systems for which the key was a symmetric function of degree two, but these were insecure. Shamir's signature scheme [38], cryptanalyzed by Coppersmith and Stern, also uses symmetric functions. Our results suggest that cyclic functions still have some use in cryptography. Although it is hard for an adversary to compute the session key, it is not clear which bits of this key are hard. Since this problem is also open for the Diffie-Hellman key exchange, it is beyond the scope of this paper.
Our scheme does not require a chair whose cost will be higher than the other participants. Furthermore the number of rounds required is independent of the number of conference participants (and small [4, 17]).

To achieve security against active adversaries we have extended our conference key distribution protocol. Users have a public key and authenticate their messages using an appropriate authentication scheme. The resulting system is proven secure against an active attack under the same assumptions as before, while remaining practical.

The authentication used in our protocol is only proven secure against a (chosen independently) known plaintext attack (which is sufficient for the security of the conference key system). We have extended our authentication system so that it is also proven secure against an adaptive chosen text attack by a real time middle-person provided the discrete logarithm problem is intractable. This resulting scheme remains practical.

References


