

***** COVER PAGE *****

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.

***** COVER PAGE *****

*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, 25, 8, 6, 31, 27, 32]). Research has focused on security and on efficiency. Many practical systems have been proposed [31, 27, 32, 38, 39, 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 [25, 26, 32, 38, 20, 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 [25]. 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 [23]) 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 [23, 29, 35, 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 [34], 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 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 networks² in which the users U_i can *broadcast* ‘messages’ (strings) to each other. We allow for the possibility that an eavesdropper³ E (a malicious adversary) may read the broadcast messages or substitute some of them. We distinguish two types of networks: those for which E is passive and those for which E is active. Let N be the security parameter.

Definition 1. Suppose that $n = O(N^c)$, $c > 0$ constant, interactive Turing machines U_1, \dots, 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, \dots, 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, \dots, 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 tape) which corresponds to its public key k_i , which is published. Let $n' > 0$ of these be honest⁴, $n'' = n - n' \geq 0$ be impersonators⁴, 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'_1 ,
- *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, α, β and γ , find $\beta^{\log_{\alpha} \gamma} \bmod p$ if it exists.

Breaking this problem has remained an open problem for more than 15 years. Even if the factorization of the order of α is known the problem is assumed to be hard (cf. [9, 11, 12]). It is well known [30, 16, 28, 24] that if the Discrete Logarithm problem is easy then so is the Diffie-Hellman problem, but the converse may not be true.

²A 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.

³An 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.

⁴An 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_i with the help of an impersonator (if there is one). We will strengthen the definition in the final paper.

3 A conference key distribution system

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

Protocol 1. Let U_1, \dots, U_n be a (dynamic) subset of all users⁵ who want to generate a common conference key.

MOVE 1. Each U_i , $i = 1, \dots, n$, selects⁶ $r_i \in_R Z_q$, computes and broadcasts $z_i = \alpha^{r_i} \pmod{p}$.

MOVE 2. Each U_i , $i = 1, \dots, n$, checks⁷ that $\alpha^q \equiv 1 \pmod{p}$ and that $(z_j)^q \equiv 1 \pmod{p}$ for all $j = 1, \dots, n$, and then computes and broadcasts

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

where the indices are taken in a cycle.

MOVE 3. Each U_i , $i = 1, \dots, n$, computes the conference key,

$$K_i \equiv (z_{i-1})^{nr_i} \cdot X_i^{n-1} \cdot X_{i+1}^{n-2} \cdots X_{i-2} \pmod{p}.$$

Remark 2. Honest users compute the same key,

$$K \equiv \alpha^{r_1 r_2 + r_2 r_3 + \cdots + r_n r_1} \pmod{p}.$$

Indeed, set $A_{i-1} \equiv (z_{i-1})^{r_i} \equiv \alpha^{r_i r_{i-1}} \pmod{p}$, $A_i \equiv (z_{i-1})^{r_i} \cdot X_i \equiv \alpha^{r_i r_{i-1} + r_i} \pmod{p}$, $A_{i+1} \equiv (z_{i-1})^{r_i} \cdot X_i \cdot X_{i+1} \equiv \alpha^{r_i r_{i-1} + r_i + r_{i+1}} \pmod{p}$, etc., and we have $K_i = A_{i-1} \cdot A_i \cdot A_{i+1} \cdots A_{i-2}$. So the key is a second order cyclic function of the r_i (but not symmetric as in [25]).

For $n = 2$ we get $X_1 = X_2 = 1$ and $K \equiv \alpha^{r_1 r_2 + r_2 r_1} \equiv \alpha^{2r_1 r_2} \pmod{p}$, 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 $K_1 \equiv (z_n)^{nr_1} \cdot X_1^{n-1} \cdot X_2^{n-2} \cdots X_{n-1} \pmod{p}$ 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, \dots, b_{n-1} at random from Z_q , and compute:

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

Since n is even we must also have,

$$\begin{aligned} z_n &\equiv z_2 \cdot \alpha^{-b_2} &\equiv z_4 \cdot \alpha^{-b_2 - b_4} &\equiv \dots &\equiv z_{n-2} \cdot \alpha^{-b_2 - b_4 - \dots - b_{n-2}} \pmod{p}, \\ z_1 &\equiv z_3 \cdot \alpha^{-b_3} &\equiv z_5 \cdot \alpha^{-b_3 - b_5} &\equiv \dots &\equiv z_{n-1} \cdot \alpha^{-b_3 - b_5 - \dots - b_{n-1}} \pmod{p}. \end{aligned} \quad (2)$$

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, \dots, X_{n-2} . Using (2), $X_{n-1} \equiv (z_n/z_{n-2})^{r_{n-1}} \equiv (z_{n-1})^{-b_2 - b_4 - \dots - b_{n-2}} \pmod{p}$, and $X_n \equiv (z_1/z_{n-1})^{r_n} \equiv (z_n)^{-b_3 - b_5 - \dots - b_{n-1}} \pmod{p}$. 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, \dots, z_{n-1} and the computed X_1, \dots, X_n . From our assumption, E will obtain the corresponding K_1 .

⁵An abuse of notation: there may be more than n users altogether.

⁶We use the notation $a \in_R A$ to indicate that a is selected from the set A uniformly and independently.

⁷If the center is trusted (oracle) the first test is not required.

Clearly E can easily compute $(z_n)^{nr_1} \bmod p$ from K_1 . It is well known [7, 33] that it is feasible to compute n -th residues in Z_p when n is polynomially bounded. E may not be able to find which one corresponds to $(z_n)^{r_1} \bmod p$, 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 $(z_n)^{r_1} \bmod p$. So we have a violation of the intractability of the Diffie-Hellman problem. \square

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. \square

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 , α and q , but now q is a prime. Then each user P selects $a, b \in_R Z_q$, computes $\beta = \alpha^a \bmod p$, $\gamma = \alpha^b \bmod p$, and registers $k = (\beta, \gamma)$ as its public key.⁸

Protocol 2. *Common input: $(p, \alpha, q, \beta, \gamma)$.*

P has a, b written on the knowledge tape, where $\beta = \alpha^a \bmod p$, $\gamma = \alpha^b \bmod p$. P is given $z \in Z_q$.

P authenticates z to V : P sends z to V and then proves to V that it knows the discrete logarithm of $\beta^z \gamma \bmod p$ ($= az + b \bmod q$), by using any interactive zero-knowledge proof of knowledge (e.g., [15, 14, 4, 17]). V verifies this and checks⁷ that $\alpha \not\equiv 1 \pmod{p}$, $\alpha^q \equiv \beta^q \equiv \gamma^q \equiv 1 \pmod{p}$ 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 ($z \in Z_q$ is chosen independently of γ) if the order of α 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 proofs⁹, is accepted by the verifier with non-negligible probability. From the definition of soundness¹⁰ for proofs of knowledge [19, 1] it follows that P' must know $az + b \bmod q$. P' is now used as a black box to break the Discrete Logarithm of γ . Take as common input $(p, \alpha, q, \alpha^r, \gamma)$, where $r \in_R Z_q$. The history h can easily be simulated. Then give the common input and h to P' to get: $z \in Z_q$ and $rz + DL(\gamma) \bmod q$. 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 $az + b \bmod q$ to a proof $({}^P P', V)$ of knowledge of $az' + b \bmod q$, $z' \neq z$ (after having observed earlier proofs). We shall show that ${}^P P'$ can be used to break the Discrete Logarithm problem of β . Assume that P has $az + b \bmod q$ on its knowledge tape (*only*, not a, b). As in the previous case, ${}^P P'$ must know $az' + b \bmod q$. Choose $r \in_R Z_q$ (r replaces $az + b$), $z \in Z_q$, and history

⁸There is no need for p, q to be standard.

⁹These earlier proofs are proofs (P, V) of knowledge of $az_i + b$, and proofs (P, P', V) in which (P, P') have used (k, z_j) and (P', V) have used (k, z'_j) .

¹⁰Important technical remarks about proofs of knowledge were discussed in [1]. In the final paper we discuss these issues in our context.

h , and let $\gamma \equiv \alpha^r \beta^{-z} \pmod{p}$. So z must be independently of γ (otherwise we could not take r to be random). Then input to ${}^P P'$: $(p, \alpha, q, \beta, \gamma)$, z , h , and put r on the knowledge tape of P , to get: z' and $DL(\beta)z' + DL(\gamma) \equiv DL(\beta)(z' - z) + r \pmod{q}$. Since z', z, r are known, it is easy to compute $DL(\beta)$ when $z' \neq z$. \square

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.

5 An authenticated conference key

Theorem 3. *Let p_1, α_1 and q_1 be as in Section 3, and p_2, α_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, α_2, q_2 and public key $k_i = (\beta_2, \gamma_2)$, before Step 3 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 $(z_n)^{r_1} \pmod{p}$. 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 $(z_n)^{r_1} \pmod{p}$, knowing only $z_1 = \alpha^{r_1} \pmod{p}$ 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 γ 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, α_2, q_2) , (p_3, α_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 $\beta_2 = \alpha_2^{a_2} \pmod{p_2}$, $\beta_3 = \alpha_3^{a_3} \pmod{p_3}$, $\gamma_3 = \alpha_3^{b_3} \pmod{p_3}$, $a_2 \in_R Z_{q_2}$, $a_3, b_3 \in_R Z_{q_3}$. The following protocol is used to authenticate any number $z \in Z_{q_2}$:

Protocol 3. *Common input:* $(p_2, \alpha_2, q_2, p_3, \alpha_3, q_3; \beta_2, \beta_3, \gamma_3)$.

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

P authenticates z to V : P sends to V : z and $\gamma_2 = \alpha_2^{b_2} \pmod{p_2}$, where $b_2 \in_R Z_{q_2}$, and then proves to V , simultaneously, that it knows the discrete logarithm base α_2 of $\beta_2^z \cdot \gamma_2 \pmod{p_2}$ ($= a_2 z + b_2 \pmod{q_2}$), and the discrete logarithm base α_3 of $\beta_3^{\gamma_2} \cdot \gamma_3 \pmod{p_3}$ ($= a_3 \gamma_2 + b_3 \pmod{q_3}$), by using a zero-knowledge proof of knowledge (*e.g.*, [15, 14, 4, 17]).

V verifies this, checks that $\gamma_2^{q_2} \equiv 1 \pmod{p_2}$, and then checks⁷ that $\alpha \not\equiv 1 \pmod{p}$, $\alpha_2^{q_2} \equiv \beta_2^{q_2} \equiv 1 \pmod{p_2}$, $\alpha_3^{q_3} \equiv \beta_3^{q_3} \equiv \gamma_3^{q_3} \equiv 1 \pmod{p_3}$ 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 $A_2 \equiv a_2 z + b_2 \pmod{q_2}$ and $A_3 \equiv a_3 \gamma_2 + b_3 \pmod{q_3}$ (z is chosen by P'), to a proof $({}^P P', V)$ of knowledge of $a_2 z' + b_2 \pmod{q_2}$ and $a_3 \gamma_2' + b_3 \pmod{q_3}$, with $z' \neq z$, after having observed earlier proofs. Then ${}^P P'$ must know both $a_2 z' + b_2' \pmod{q_2}$ and $a_3 \gamma_2' + b_3 \pmod{q_3}$, where

$\gamma'_2 = \alpha_2^{b'_2} \bmod p_3$. We shall use ${}^P P'$ to break the Discrete Logarithm problem. We distinguish two cases, which we run each with probability one half.

Case 1: $\gamma'_2 \equiv \gamma_2 \pmod{p_2}$. Take $\delta_2 \in_R \langle \alpha_2 \rangle$ (δ_2 replaces β_2) as an instance for the Discrete Logarithm problem and choose $a_3, b_3 \in_R Z_{q_3}$, and compute $\beta_3 = \alpha_3^{a_3} \bmod p_3$, $\gamma_3 = \alpha_3^{b_3} \bmod p_3$. For any given $z \in Z_{q_2}$ take $r_2 \in_R Z_{q_2}$ (r_2 replaces $a_2 z + b_2 \bmod q_2$), and compute $\gamma_2 = \alpha_2^{r_2} \delta_2^{-z} \bmod p_2$ and $r_3 = a_3 \gamma_2 + b_3 \bmod q_3$, and a simulated history h . Then input to ${}^P P'$: $(\delta_2, \beta_3, \gamma_3), z, h$, and put r_2, r_3 on the knowledge tape of P , to get: z' and γ'_2, A'_2, A'_3 . If $\gamma'_2 \equiv \gamma_2 \pmod{p_2}$ then $A'_2 \equiv DL(\delta_2)z' + DL(\gamma_2) \equiv DL(\delta_2)(z' - z) + r_2 \pmod{q_2}$, and since $z' \neq z$ we get $DL(\delta_2)$. Else ignore.

Case 2: $\gamma'_2 \not\equiv \gamma_2 \pmod{p_2}$. Take $\delta_3 \in_R \langle \alpha_3 \rangle$ (δ_3 replaces β_3) as an instance for the Discrete Logarithm problem, and $r_3 \in_R Z_{q_3}$ (r_3 replaces $a_3 \gamma_2 + b_3 \bmod q_3$) and choose $a_2, b_2 \in_R Z_{q_2}$, and compute $\beta_2 = \alpha_2^{a_2} \bmod p_2$, $\gamma_2 = \alpha_2^{b_2} \bmod p_2$, and $\gamma_3 \equiv \alpha_3^{r_3} \cdot \delta_3^{-\gamma_2} \bmod p_3$. Input to P' : $(\beta_2, \delta_3, \gamma_3)$, which chooses $z \in Z_{q_2}$. Compute $r_2 = a_2 z + b_2 \bmod q_2$, and history h . Then input to ${}^P P'$: $(\beta_2, \delta_3, \gamma_3), z, h$, and put r_2, r_3 on the knowledge tape of P , to get: $z', \gamma'_2, A'_2, A'_3$. If $\gamma'_2 \not\equiv \gamma_2 \pmod{p_2}$ then $A'_3 \equiv DL(\delta_3)\gamma'_2 + DL(\gamma_3) \equiv DL(\delta_3)(\gamma'_2 - \gamma_2) + r_3 \bmod q_3$, and we get $DL(\delta_3)$. Else ignore. \square

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 [37], 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

- [1] M. Bellare and O. Goldreich. On defining proofs of knowledge. In E. F. Brickell, editor, *Advances in Cryptology — Crypto '92, Proceedings (Lecture Notes in Computer Science 740)*, pages 390–420. Springer-Verlag, 1993. Santa Barbara, California, U.S.A., August 16–20.
- [2] M. Bellare and S. Goldwasser. New paradigms for digital signatures and message authentication based on non-interactive zero-knowledge proofs. In G. Brassard, editor, *Advances in Cryptology — Crypto '89, Proceedings (Lecture Notes in Computer Science 435)*, pages 194–211. Springer-Verlag, 1990. Santa Barbara, California, U.S.A., August 20–24.
- [3] M. Bellare and S. Micali. How to sign given any trapdoor function. *Journal of the ACM*, 39(1):214–233, January 1992.
- [4] M. Bellare, S. Micali, and R. Ostrovsky. Perfect zero-knowledge in constant rounds. In *Proceedings of the twenty second annual ACM Symp. Theory of Computing, STOC*, pages 482–493, May 14–16, 1990.

- [5] S. Bengio, G. Brassard, Y. G. Desmedt, C. Goutier, and J.-J. Quisquater. Secure implementations of identification systems. *Journal of Cryptology*, 4(3):175–183, 1991.
- [6] C. H. Bennett and G. Brassard. Quantum cryptography, and its application to provable secure key expansion, public-key distribution, and coin tossing. In *International Symposium on Information Theory (abstracts)*, page 91. IEEE, September 26–30, 1983. St. Jovite, Quebec, Canada.
- [7] E. R. Berlekamp. Factoring polynomials over large finite fields. *Mathematics of Computation*, 24(111):713–735, 1970.
- [8] R. Blom. Key distribution and key management. In *Proc. Eurocrypt 83*, Udine, Italy, March 1983.
- [9] M. Blum and S. Micali. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM J. Comput.*, 13(4):850–864, November 1984.
- [10] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly-secure key distribution for dynamic conferences. In E. F. Brickell, editor, *Advances in Cryptology — Crypto '92, Proceedings (Lecture Notes in Computer Science 740)*, pages 471–486. Springer-Verlag, 1993. Santa Barbara, California, U.S.A., August 16–20.
- [11] J. Boyar, M.W. Krentel, and S.A. Kurtz. A discrete logarithm implementation of zero-knowledge blobs. Technical Report 87-002, University of Chicago, March 1987.
- [12] G. Brassard, D. Chaum, and C. Crépeau. Minimum disclosure proofs of knowledge. *Journal of Computer and System Sciences*, 37(2):156–189, October 1988.
- [13] J. L. Carter and M. N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18:143–154, 1979.
- [14] D. Chaum, J.-H. Evertse, and J. van de Graaf. An improved protocol for demonstrating possession of discrete logarithms and some generalizations. In D. Chaum and W. L. Price, editors, *Advances in Cryptology — Eurocrypt '87 (Lecture Notes in Computer Science 304)*, pages 127–141. Springer-Verlag, Berlin, 1988. Amsterdam, The Netherlands, April 13–15, 1987.
- [15] D. Chaum, J.-H. Evertse, J. van de Graaf, and R. Peralta. Demonstrating possession of a discrete logarithm without revealing it. In A. Odlyzko, editor, *Advances in Cryptology. Proc. of Crypto '86 (Lecture Notes in Computer Science 263)*, pages 200–212. Springer-Verlag, 1987. Santa Barbara, California, U.S.A., August 11–15.
- [16] D. Coppersmith, A. Odlyzko, and R. Schroepfel. Discrete logarithms in $GF(p)$. *Algorithmica*, pages 1–15, 1986.
- [17] Y. Desmedt and M. Burmester. An efficient zero-knowledge scheme for the discrete logarithm based on smooth numbers. In H. Imai, R. L. Rivest, and T. Matsumoto, editors, *Advances in Cryptology — Asiacrypt '91, Proceedings (Lecture Notes in Computer Science 739)*, pages 360–367. Springer-Verlag, 1993. Fujiyoshida, Japan, November, 1991.
- [18] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, IT-22(6):644–654, November 1976.
- [19] U. Feige, A. Fiat, and A. Shamir. Zero knowledge proofs of identity. *Journal of Cryptology*, 1(2):77–94, 1988.
- [20] M. J. Fischer and R. N. Wright. Multiparty secret key exchange using a random deal of cards. In J. Feigenbaum, editor, *Advances in Cryptology — Crypto '91, Proceedings (Lecture Notes in Computer Science 576)*, pages 141–155. Springer-Verlag, 1992. Santa Barbara, California, U.S.A., August 12–15.
- [21] Z. Galil, S. Haber, and M. Yung. A private interactive test of a Boolean predicate and minimum-knowledge public key cryptosystems. In *Annual Symp. on Foundations of Computer Science (FOCS)*, pages 360–371, 1985.
- [22] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208, February 1989.
- [23] S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. Comput.*, 17(2):281–308, April 1988.
- [24] D. Gordon. Discrete logarithm in $GF(p)$ using the number field sieve. Submitted.
- [25] I. Ingemarsson, D. T. Tang, and C. K. Wong. A conference key distribution system. *IEEE Trans. Inform. Theory*, 28(5):714–720, September 1982.

- [26] K. Koyama and K. Ohta. Identity-based conference key distribution systems. In C. Pomerance, editor, *Advances in Cryptology, Proc. of Crypto '87 (Lecture Notes in Computer Science 293)*, pages 175–185. Springer-Verlag, 1988. Santa Barbara, California, U.S.A., August 16–20.
- [27] K. S. McCurley. A key distribution system equivalent to factoring. *Journal of Cryptology*, 1(2):95–105, 1988.
- [28] A. Menezes, S. Vanstone, and T. Okamoto. Reducing elliptic curve logarithms to logarithms in a finite field. In *Proceedings of the Twenty third annual ACM Symp. Theory of Computing, STOC*, pages 80–89, 1991.
- [29] M. Naor and M. Yung. Universal one-way hash functions and their cryptographic applications. In *Proceedings of the twenty first annual ACM Symp. Theory of Computing, STOC*, pages 33–43, May 15–17, 1989.
- [30] A. M. Odlyzko. Discrete logs in a finite field and their cryptographic significance. In N. Cot T. Beth and I. Ingemarsson, editors, *Advances in Cryptology, Proc. of Eurocrypt 84 (Lecture Notes in Computer Science 209)*, pages 224–314. Springer-Verlag, 1984. Paris, France April 1984.
- [31] E. Okamoto. Key distribution systems based on identification information. In C. Pomerance, editor, *Advances in Cryptology, Proc. of Crypto '87 (Lecture Notes in Computer Science 293)*, pages 194–202. Springer-Verlag, 1988. Santa Barbara, California, U.S.A., August 16–20.
- [32] E. Okamoto and K. Tanaka. Key distribution system based on identification information. *IEEE J. Selected Areas in Commun.*, 7(4):481–485, 1989.
- [33] M. Rabin. Probabilistic algorithms in finite fields. *SIAM Journal on Computing*, 9(2):273–280, 1980.
- [34] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Commun. ACM*, 21:294–299, April 1978.
- [35] J. Rompel. One-way functions are necessary and sufficient for secure signatures. In *Proceedings of the twenty second annual ACM Symp. Theory of Computing, STOC*, pages 387–394, May 14–16, 1990.
- [36] A. W. Schrifft and A. Shamir. The discrete log is very discreet. In *Proceedings of the twenty second annual ACM Symp. Theory of Computing, STOC*, pages 405–415, May 14–16, 1990.
- [37] A. Shamir. Efficient signature schemes based on birational permutations. In D. R. Stinson, editor, *Advances in Cryptology — Crypto '93, Proceedings (Lecture Notes in Computer Science 773)*, pages 1–12. Springer-Verlag, 1994. Santa Barbara, California, U.S.A., August 22–26.
- [38] S. Tsujii and T. Itoh. An ID-based cryptosystem based on the discrete logarithm. *IEEE J. Selected Areas in Commun.*, 7:467–473, 1989.
- [39] P. C. van Oorschot W. Diffie and M. J. Wiener. Authentication and authenticated key exchanges. *Designs, Codes and Cryptography*, 2:107–125, 1992.
- [40] M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22:265–279, 1981.
- [41] Y. Yacobi and Z. Shmueli. On key distribution systems. In G. Brassard, editor, *Advances in Cryptology — Crypto '89, Proceedings (Lecture Notes in Computer Science 435)*, pages 344–355. Springer-Verlag, 1990. Santa Barbara, California, U.S.A., August 20–24.