Secure group communication using fractional public keys

Sigurd Eskeland and Vladimir Oleshchuk

University of Agder
Grooseveien 36
N-4876 Grimstad, Norway
{sigurd.eskeland, vladimir.oleshchuk}@uia.no

Abstract

In this paper, we present the novel concept of fractional public keys and an efficient zero-round multi-party Diffie-Hellman key agreement scheme that is based on fractional public keys. Shared group keys are computed highly efficiently by using the fractional public keys of multiple participants as exponents. The scheme provides therefore an efficient and elegant way of multi-party key agreement without key establishment data transmissions. The presented cryptographic scheme is collusion resistant to any number of users.

1 Introduction

The simple and elegant two-party key agreement scheme of Diffie and Hellman has to a large extent gotten the credit for introducing the concept of public key cryptography. The scheme has been the basis for a relatively large number of cryptographic protocols. Since it lacks user authentication, a number of these schemes provide user authentication. Diffie-Hellman (DH) key agreement is also the basis for a number of group-oriented key agreement schemes known as conference key agreement protocols. A common characteristic of the schemes of this class of cryptographic protocols is that they have a varying degree of efficiency in terms of the number of rounds of message transmissions and the number of computations and exponentiations for each participant.

In this paper, we introduce a new approach for secure group key computation that is in agreement with the Diffie-Hellman key agreement paradigm, and that is mostly beneficial concerning efficiency and elegancy. In contrast to using public keys computed as exponentiations, our scheme uses public keys that are computed on a fractional form. The fractional public keys are used as exponents for computing group keys according to a modified version of the Diffie-Hellman scheme. Since public user keys are used as exponents, any number of public keys can be used simultaneously, meaning that the presented scheme is a true multi-party shared key establishment scheme providing convenient and efficient group-oriented key agreement. Since the value of the group key is based on the long-term public keys of the participants, no data transmissions are required. The scheme hence provides zero-round multi-party Diffie-Hellman key agreement.

1.1 Related work

The concept of fractional public keys is influenced by the cryptographic scheme proposed in [5]. In this paper, a collusion resistant threshold cryptosystem is proposed by using private user keys (user shares) that is computed on a fraction form, where the numerator and denominator are secret polynomials. As will be subsequently shown, fractional public keys provide an efficient secure group key computation.

Public key cryptography has been credited W. Diffie and M. Hellman for their classical two-party key agreement scheme from 1976 [4]. This scheme has since been used as basis for great number of subsequent cryptographic schemes. The lack of user and/or key authentication in the original Diffie-Hellman (DH) scheme has caused the proposal of many extended DH schemes. These are basically key agreement protocols with user authentication, and some others are user authentication protocols. An interesting overview over this family of cryptographic schemes can be found in Chapter 5 of [2].

Although the DH scheme is a two-party protocol, some authors have proposed generalizations of the DH scheme for conference key agreement (CKA). An early unauthenticated DH-CKA protocol was proposed by Ingemarsson et al. [6]. This scheme has a relatively high overhead concerning computation and the number of transmitted messages. Steiner et al. [11] presented three protocols named GDH.1, GDH.2 and GDH.3, which can be regarded as variations of [6]. They are more efficient concerning the number of

computations and transmitted messages, but require more rounds than [6].

Burmester and Desmedt [3] proposed an elegant multi-party generalization of DH, which provides relatively high efficiency, and requires only 2 rounds and 3 exponentiations. Since each user broadcasts the message of the second round to the others, it is highly suitably for wireless networks.

Identity-based authenticated protocols have among others been proposed by Koyoma and Otha [7, 8], and Saeednia and Safavi-Naini whose DH-CKA protocol [10] is based on the Burmester-Desmedt protocol [3]. Ateniese et al. [1] extended the GDH.2 scheme [11] for user authentication. Also see Chapter 6 of [2] for an excellent overview of DH-CKA protocols and for comparisons.

2 Zero-round multi-party Diffie-Hellman key agreement from fractional public keys

In this section, we present the new cryptographic group-oriented key computation scheme. It consists of an initialization phase requiring a trusted party providing each user with a public/private long-term user key pair. The group keys are computed as a function of the long-term user keys of any given user coalition. Each user can therefore compute group keys offline for any user coalition the given user is a member of, without computing and transmitting key establishment messages.

Initialization. A Trusted Authority (TA) selects two large secret primes p and q, where the product $n = p \cdot q$ is public. According to the RSA public key cryptosystem [9], the TA selects a public number e that is relatively prime to $\phi(n) = (p-1) \cdot (q-1)$, and computes a secret number d so that $e \cdot d \equiv 1 \pmod{\phi(n)}$. A public element α of high order in $\mathbb{Z}_n^*$ is also selected.

Let $\mathcal{U}$ denote a group of an arbitrary number of users, where $T \subseteq \mathcal{U}$ denotes an arbitrary user subset. The cryptosystem allows all members of $T \subseteq \mathcal{U}$ to securely compute a shared secret group key. Hence, the scheme provides secure multi-party key agreement with the advantage that secret group keys can be computed without user interaction and key establishment data transmissions.

Public/private user key computation. The TA generates for each participant $P_i \in \mathcal{U}$ a random secret number $x_i \in \mathbb{Z}_{\phi(n)}$. The TA selects for each $P_i \in \mathcal{U}$ a public number I_i, so that $(d + I_i)$ is relatively prime to $\phi(n)$. The public I_i could for example represent a meaningful identity of P_i.

The TA computes the public key for $P_i \in \mathcal{U}$ as

$$y_i = \frac{x_i}{d + I_i} \pmod{\phi(n)}$$

and the corresponding private key

$$k_i = \alpha^{x_i \cdot d^{M-1}} \pmod{n}$$

where M denotes the maximum possible size of any user coalition T. (The coalition max size must consequently be the same as or less than the total number of users assigned such long-term user keys.) The private key k_i is transmitted to $P_i \in \mathcal{U}$ through a secure channel.

Group key computation. At this stage, the participants of a user coalition $T \subseteq \mathcal{U}$ compute the shared group key K_T according the following method:
Let $I_{T,i} = \{j \,|\, P_j \in T \backslash \{P_i\}\}$. Let $t = |T|$. Given a polynomial

$$g_i(d) = \prod_{j \in I_{T,i}} (I_j + d)$$

each participant $P_i \in T$ computes the corresponding polynomial coefficients $c_{i,j}$, $0 \leq j \leq t-1$, so that

$$g_i(d) = \sum_{j=0}^{t-1} c_{i,j} \cdot d^j$$

Note that the values of $c_{i,j}$ are independent of the value of the secret d. It can also be noted as a matter of form that the value of d is fixed although $g_i(d)$ refers to a polynomial.
For $j \in \{0, \ldots, t-1\}$, let

$$\begin{aligned} w_{i,j} &= k_i^{e^{M-1-j}} \pmod{n} \\ &= (\alpha^{x_i \cdot d^{M-1}})^{e^{M-1-j}} \pmod{n} \\ &= \alpha^{x_i \cdot d^{M-1} \cdot d^{-M+1+j}} \pmod{n} \\ &= \alpha^{x_i \cdot d^j} \pmod{n} \end{aligned}$$

Each $P_i \in T$ computes the secret group key K_T for that coalition $T \subseteq \mathcal{U}$ according to

$$\begin{aligned} K_T &= \Big(\prod_{j=0}^{t-1} w_{i,j}^{c_{i,j}}\Big)^{\prod_{j \in I_{T,i}} y_j} \pmod{n} \\ &= \Big(\prod_{j=0}^{t-1} \alpha^{x_i \cdot d^j \cdot c_{i,j}}\Big)^{\prod_{j \in I_{T,i}} y_j} \pmod{n} \\ &= \Big(\alpha^{x_i \cdot \prod_{j \in I_{T,i}} (d+I_j)}\Big)^{\prod_{j \in I_{T,i}} \frac{x_j}{d+I_j}} \pmod{n} \\ &= \alpha^{\prod_{j \in I_T} x_j} \pmod{n} \end{aligned}$$

where $I_T = \{j \,|\, P_j \in T\}$.

3 Security analysis

In this section, we present the relevant security assumptions and security requirements of the presented scheme, and then we show that the actual security of the scheme is in agreement with the given security requirements.

3.1 Security requirements

We assume that there exists a set $\mathcal{U}$ of an arbitrary number of users. A group key K_T is computed as a function of the long-term user keys of any user subset $T \subseteq \mathcal{U}$. It can be assumed an adversary A that is equivalent with a user coalition $A \subseteq \mathcal{U}$, where $A \cap T = \emptyset$ for any coalition $T \subseteq \mathcal{U}$.

Adversary assumptions. We assume that A may hold the following information:

- The private user keys $k_i = \alpha^{x_i \cdot d^{M-1}} \pmod n$ for each $P_i \in A$.
- The group keys $K_{T^*} = \alpha^{\prod_{j|P_j \in T^*} x_j} \pmod n$ for any $T^* \subseteq \mathcal{U}$, where $T^* \neq T$.
- The public user key y_i for each $P_i \in \mathcal{U}$.

Security requirements. There is no communication required to compute group keys K_T, which are computed as a function of the long-term user keys of the user coalition $T \subseteq \mathcal{U}$. Data to be communicated confidentially is encrypted by means of a secure symmetric key cryptographic algorithm using the secret group key as cryptokey. Assuming that the symmetric key cryptographic algorithm used is secure, the security of the scheme is based on the difficulty for an adversary (or coalition of adversaries) A, to violate the following security requirements:

Security Requirement 1. *Secrecy of private keys.* It must be computationally infeasible to obtain private user keys.

Security Requirement 2. *Secrecy of group keys.* No other than the members of a given coalition $T \subseteq \mathcal{U}$ must be able to compute the shared secret group key K_T corresponding to the long-term user keys of the given participants.

Security Requirement 3. *Coalition resistance.* It must be prevented that any colluding user coalition $A \subseteq \mathcal{U}$ may violate the two former security requirements.

The security of the presented scheme is based on the secrecy of $\phi(n)$, d and x_j (for any $P_i \in \mathcal{U}$). We will now in this regard present some relevant observations:

Observation 1. Secrecy of the secret parameters d and x_j (for any $P_i \in \mathcal{U}$) concerning fractional public keys. The public keys are computed according to

$$y_i = \frac{x_i}{d + I_i} \pmod{\phi(n)}$$

which corresponds to the equation

$$x_i = y_i \cdot d + y_i \cdot I_i \Leftrightarrow y_i \cdot I_i = x_i - y_i \cdot d$$

Since d and x_i (for each y_i) are unknown, the equation system is underdefined and can clearly not be solved, thereby effectively prohibiting deduction of the secret x_i and d. Accordingly, two or more y_j correspond likewise to underdefined linear equation systems, which hence cannot be solved.

Observation 2a. Secrecy of the secret parameters d and x_j (for any $P_i \in \mathcal{U}$) concerning private keys. Regarding the private key $k_i = \alpha^{x_i \cdot d^{M-1}} \pmod n$ (and hence the corresponding $w_{i,j} = \alpha^{x_i \cdot d^j} \pmod n$), the secret d and x_i are accordingly protected due to the Discrete Logarithm Problem.

Observation 2b. Secrecy of x_j (for any $P_j \in \mathcal{U}$) concerning group keys. Regarding the group key $K_T = \alpha^{\prod_{j|P_j \in T} x_j} \pmod n$, the secret x_i (for any $P_i \in \mathcal{U}$) is accordingly protected due to the Discrete Logarithm Problem.

Observation 2c. The secrecy of d given the public e and n is in agreement with the RSA public key cryptosystem [9].

Observation 3. Let $W_j = \alpha^{w^j}$. An adversary $P_i \in A$, holding the private user key $k_{i,0}$ can by means of the corresponding public user key y_i compute

$$W_1 = \alpha^d = k_{i,0}^{y_i^{-1} \bmod \phi(n)} \cdot \alpha^{-I_i} = \alpha^{x_i \cdot \frac{d+I_i}{x_i}} \cdot \alpha^{-I_i} \pmod n$$

Given W_{j-1}, $1 < j < M$, the following computations can be carried recursively out:

$$\begin{aligned} W_j &= \alpha^{d^j} = k_{i,j}^{y_i^{-1} \bmod \phi(n)} \cdot W_{j-1}^{-I_i} \pmod n \\ &= \alpha^{x_i \cdot d^j \cdot \frac{d+I_i}{x_i}} \cdot \alpha^{-d^{j-1} \cdot I_i} \pmod n \end{aligned}$$

This attack requires computation of inverses modulo $\phi(n)$. Since n is a large composite number, computing $\phi(n)$ is equivalent of solving the Factorization Problem, which is known to be computationally infeasible.

3.2 Security requirements

We will now provide the security proofs of the security requirements.

Proof of Security Requirement 1. *Security of private keys.* According to Observations 1 and 2a-c, it is infeasible to deduce both d and x_i (for any $P_i \in \mathcal{U}$) from public/private keys and group keys. Since the private keys are on the form $w_{i,j} = \alpha^{x_i \cdot d^j}$, private keys can thus not be obtained by this computation since d and x_i (for any $P_i \in \mathcal{U}$) are secret.

According to Observation 3, computation of $W_j = \alpha^{d^j} \pmod n$ (for $1 \leq j \leq M-1$) is prevented since $\phi(n)$ is unknown. Accordingly, it is computationally infeasible to obtain $W_j = \alpha^{d^j}$ given $w_{i,j} = \alpha^{x_i \cdot d^j} \pmod n$ for any $P_i \in \mathcal{U}$ due to the Discrete Logarithm Problem.

It can be noted that given W_j and W_{j+1} would allow computation of private keys according to

$$\begin{aligned} w_{i,j} &= \left(W_{j+1} \cdot W_j^{I_i}\right)^{y_i} \pmod{n} \\ &= \left(\alpha^{d^j \cdot (d+I_i)}\right)^{\frac{x_i}{d+I_i}} = \alpha^{x_i \cdot d^j} \pmod{n} \end{aligned}$$

It is therefore computationally infeasible to compute private keys by this computation without knowledge of the secret $\phi(n)$, where computing $\phi(n)$ is equivalent of solving the Factorization Problem. Thus, disclosure of private keys is prevented, and the scheme is secure in agreement with Security Requirement 1.

Proof of Security Requirement 2. *Group key security.* A group key can be computed given disclosure of the secret d, x_i (for any $P_i \in \mathcal{U}$) and $\phi(n)$, since this would enable computation of private user keys. In agreement with Security Requirement 1, an adversary is prevented to obtain any private key of users in T. The adversary is accordingly prevented from using such a key to compute the corresponding group key K_T.

Let us assume that A possesses a group key K_{T^*} for any $T^* \subseteq \mathcal{U}$, $T^* \neq T$, and a group key $K_{T^{**}}$ for any $T^{**} \subseteq \mathcal{U}$, $T^{**} \neq T$, where $T = T^* \cup T^{**}$ and $T^* \cap T^{**} = \emptyset$. Computing K_T given K_{T^*} and $K_{T^{**}}$ is hence equivalent to solving the Diffie-Hellman Problem, which is known to be computationally infeasible. Thus, disclosure of group keys is prevented, and the scheme is secure in agreement with Security Requirement 2.

Proof of Security Requirement 3. *Collusion resistance.* Regarding disclosure of numbers, where the difficulty of achieving this based on a number theoretical problem like the Factorization Problem or DLP, the number of colluding participants does not affect the hardness of such problems. This leaves the problem of solving the linear equation system corresponding to a set of any number of public user keys, as pointed out in Section 3.1, where the equation $x_i = y_i \cdot d + y_i \cdot I_i$ corresponds to the public key y_i. Accordingly, since two or more public keys y_j for $P_j \in \mathcal{U}$ correspond likewise to an underdefined linear equation system, it is not possible to solve such an equation system. The scheme is thus collusion resistant to any number of colluding parties. The scheme is therefore collusion resistant, and the scheme is secure in agreement with Security Requirement 3.

4 Conclusions

In this paper, we have presented the novel concept of fractional public keys and an efficient zero-round multiparty Diffie-Hellman key agreement scheme based on fractional public keys. The fractional keys enable public keys to be used as exponents, thereby allowing a novel variation of Diffie-Hellman key agreement with no key data transmissions.

References

[1] G. Ateniese, M. Steiner, and G. Tsudik. Authenticated group key agreement and friends. pages 17–26. ACM Press, 1998.

[2] C. Boyd and A. Mathuria. *Protocols for Authentication and Key Establishment*. Springer-Verlag, 2003.

[3] M. Burmester and Y. Desmedt. A secure and efficient conference key distribution system (extended abstract). In *EUROCRYPT*, pages 275–286, 1994.

[4] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[5] S. Eskeland and V. Oleshchuk. Collusion-resistant threshold cryptosystems. In *Proceedings of International Workshop on Coding and Cryptography, (WCC 09)*, 2009.

[6] I. Ingemarsson, D. Tang, and C. Wong. A conference key distribution system. *IEEE Transactions on Information Theory*, 28(5):714–719, 1982.

[7] K. Koyama and K. Ohta. Identity-based conference key distribution systems. In *CRYPTO '87: A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology*, pages 175–184, 1988.

[8] K. Koyama and K. Ohta. Security of improved identity-based conference key distribution systems. In *Lecture Notes in Computer Science on Advances in Cryptology-EUROCRYPT'88*, pages 11–22. Springer-Verlag, 1988.

[9] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[10] S. Saeednia and R. Safavi-Naini. Efficient identity-based conference key distribution protocols. In *ACISP '98: Proceedings of the Third Australasian Conference on Information Security and Privacy*, pages 320–331. Springer-Verlag, 1998.

[11] M. Steiner, G. Tsudik, and M. Waidner. Diffie-hellman key distribution extended to group communication. *Third ACM Conference on Computer and Communication Security*, 1996.