Constant Round Authenticated Group Key Agreement via Distributed Computation *

[1] [2]

[1] Cryptology Department, CELAR, 35174 Bruz Cedex, France
Emmanuel.Bresson@polytechnique.org
[2] Dépt. d'informatique, École normale supérieure, 75230 Paris Cedex 05, France.
Dario.Catalano@ens.fr

Abstract. A group key agreement protocol allows a set of users, communicating over a public network, to agree on a private session key. Most of the schemes proposed so far require a linear number (with respect to the number of participants) of communication rounds to securely achieve this goal. In this paper we propose a new constant-round group key exchange protocol that provides efficiency and privacy under the Decisional Diffie-Hellman assumption. Our construction is practical, conceptually simple and it is obtained by taking advantage of the properties of the El-Gamal encryption scheme combined with standard secret sharing techniques.

1 Introduction

Efficiency

* Extended abstract. A full version of this paper can be found at www.di.ens.fr/~catalano.

contributory

privacy

active

? ? ? ?

shared

privately

? ?

Related work –

? *et al* ?

? ?

?

et al. ? ? ?

group Diffie-Hellman assumptions ?

[1] ?

?

[1] These assumptions make use of "multiple-decker" exponents, and are not easily related to DH.

?

et al. *et al* ?

?

?

à la

$(n+1)$ $2n$

n n

$O(3n)$

Our contributions –

2

solely

2 The model

Players and network – n P_1 P_n

A

B A B

B

Adversary –

$\mathcal{A}$

$\mathcal{A}$

any

[2]

Rushing attacks –

does not

rushing

completely honest

Security notions –

[2] More precisely, $\mathcal{A}$ cannot access the storage of the session key; when considering forward-secrecy, one may consider that $\mathcal{A}$ *partially* corrupts the private memory of a player, and gets the long-term key.

implicit authentication

explicit authentication

Notations – ℓ $\mathbb{N}$ $\mathbb{R}^+$ $\mathsf{negl} : \mathbb{N} \to \mathbb{R}^+$ *negligible* $\rho(\ell)$ $\ell_0 \in \mathbb{N}$ $\ell > \ell_0$ $\mathsf{negl}(\ell) \leq 1/\rho(\ell)$ $a, b \in \mathbb{N}$ $a|b$ a b A $a \leftarrow A$ a A A

2.1 The formal model

Players – *instances* *oracles* sk_i^t P_i t

Adversarial capabilities – $\mathcal{A}$ *queries* Send Reveal $\mathcal{A}$ sk_i^t Corrupt L_i Test $\mathcal{A}$

Necessary conditions – *Freshness* Reveal *accepted* Test Test *any* Corrupt Test Test

Reveal Test

Definitions – $\mathcal{A}$ *disrupts* $\mathcal{A}$ $\mathcal{A}$ *corrupts* L_i P_i $\mathcal{A}$

Completeness: $\mathcal{A}$ t sk^t $i \in \{1, \ldots, n\}$ $sk_i^t = sk^t$

Contributory (uniformity): $\mathcal{A}$ sk $\mathcal{K}$

Privacy: $\mathcal{B}$ κ_1 Test $\mathcal{B}$ κ_0 $\mathcal{K}$ κ_0 κ_1 $\mathcal{A}$ b *private* sk negl ℓ

$$\mathsf{Adv}(\mathcal{A}) = 2\left(\Pr\left[\mathcal{A}(\mathcal{V}, \kappa_b) = b \,\middle|\, \begin{array}{c}\kappa_0 \leftarrow \mathcal{K};\quad \kappa_1 = sk \\ b \leftarrow \{0,1\}\end{array}\right] - \frac{1}{2}\right) = \mathsf{negl}(\ell)$$

Assumption 1 (DDH Assumption) *Let p and q two primes such that $|q| = \ell$ and $q|p-1$ and g an element of order q in $\mathbb{Z}_p^\star$. Let $Q = \langle g \rangle$. There exists a negligible function* negl *such that for sufficiently large ℓ, for any probabilistic polynomial-time distinguisher Δ, we have:*

$$\mathsf{Adv}^{\mathsf{ddh}}(\Delta) = \left|\Pr_{x,y}\left[\Delta(g, g^x, g^y, g^{xy}) = 1\right] - \Pr_{x,y,z}\left[\Delta(g, g^x, g^y, g^z) = 1\right]\right| = \mathsf{negl}(\ell)$$

$X = g^x \bmod p$ $Y = g^y \bmod p$ $Z = g^{xy} \bmod p$ Q

3 The Proposed Scheme

Overview of the protocol – P_i (x_i, h_i) $h_i = g^{x_i} \bmod p$ $C_{i,j}(m, \alpha)$

m h_j α
$C_{i,j}$ P_i P_j
P_i
a_i
r_i P_i a_i
$C_{i,j}$ P_j P_i
$f_i(z)$ $n-1$ $\mathbb{Z}_q^\star$ $f_i(0) = r_i$ P_j $f_i(j)$
P_j $f_i(j)$

C_j δ_j C_j

$\delta_j \cdot a_j \bmod p$ $a = a_1 \cdots a_n \bmod p$
$f(i)$
$f_j(i)$ $f(z)$
$f(0) = r$ $r = r_1 + \ldots + r_n \bmod q$
r $f(z)$ $\mathbb{Z}_q^\star$ $sk = a \cdot g^r$

Dealing with rushing scenarios –

a_i r_i $sk = \prod_{i=1}^{n} a_i \cdot g^r \bmod p$
a_i
$sk = \prod_{i=1}^{n} a_i \bmod p$
completely
un-biaised
?? *after*

a_i

$f(i)$
r_i
r_i

all $n-1$
$n-1$

$f(\cdot)$

Authenticated Group Key Agreement Protocol

Public Parameters: Two primes p, q such that $q|p-1$. A subgroup $Q = \langle g \rangle$ of order q. An hash function $\mathcal{H}$ modeled as a random oracle, and $\mathcal{ID}$ be the current session ID.
Public inputs: The players'public keys h_i, for $i = 1, \ldots, n$.
Private input (for player i): A value x_i such that $h_i = g^{x_i} \bmod p$.
In a preprocessing stage player P_i runs a signature generation algorithm `SigGen` to obtain a couple of matching signing and verification keys (SK_i, VK_i).

First Round – Each player P_i does the following:

1. Choose $a_i \leftarrow Q$
2. Choose $r_i, b_{i,1}, \ldots, b_{i,n-1} \leftarrow \mathbb{Z}_q$.
3. Define $f_i(z) = r_i + b_{i,1}z + \ldots + b_{i,n-1}z^{n-1} \bmod q$
4. For each $j = 1 \ldots n$ $(j \neq i)$
   Choose $k \leftarrow \mathbb{Z}_q$ and set $C_{i,j} = (A_{i,j}, B_{i,j}) = (g^k \bmod p, h_j^k a_i \bmod p)$.
5. Send to player P_j the values $C_{i,j}$, $f_i(j)$ and $\sigma_{i,j} = \mathtt{Sign}_{SK_i}(C_{i,j}||f_i(j)||\mathcal{ID})$.

Second Round – Once having received all the values above each player P_i does the following: (if P_i receives less than $n-1$ triplets $(C_{j,i}, f_j(i), \sigma_{j,i})$ he aborts the protocol)

1. Check the authentication (signature) of all received values. If the check fails the player aborts the protocol.
2. Multiply the received ciphertexts: let $A_i = \prod_{j \neq i} A_{j,i} \bmod p$ and $B_i = a_i \cdot \prod_{j \neq i} B_{j,i} \bmod p$.
3. Decrypt the result to define the value $a_{(i)} = B_i / A_i^{x_i}$.
4. Compute
$$f_i = f_i(i) + \sum_{j \neq i} f_j(i) \bmod q$$
as his share of a $(n-1)$-degree polynomial $f(z)$ whose free term we indicate with r.
5. Send to other players the values f_i and $\omega_i = \mathtt{Sign}_{SK_i}(f_i||\mathcal{ID})$.

Third Round –

1. The players interpolate $f(z)$ and retrieve r.
2. Player P_i defines its session seed as
$$sk_{(i)} = a_{(i)} \cdot g^r \bmod p.$$

Confirmation Step: Compute $s_i = \mathcal{H}(sk_{(i)}||\mathcal{ID})$ and broadcast this value together with its signature $\gamma_i = \mathtt{Sign}_{SK_i}(s_i||\mathcal{ID})$.
If the n broadcasted values are all the same, set the final key as
$$sk = \mathcal{H}(sk_{(i)})$$

Fig. 1. Pseudo-code description for the Group Key Agreement Protocol

Disclosing the polynomial's shares –

Key confirmatory –

[3]

4 Security of the scheme

Theorem 1. *The protocol presented in figure* **??** *is a secure Authenticated Group Key Agreement protocol, achieving completeness, contributory and privacy (under the DDH assumption).*

Completeness –

[3] Actually the random oracle is considered for efficiency reasons only and it is not necessary for the [?] technique to work. In particular the random oracle can be replaced by a *pseudo-random* function [**?**].

Privacy – $\mathcal{S}$ *emulates*

(X, Y, Z)

$\mathcal{Q}$

$\mathcal{S}$

q_0 $[1, \mathcal{Q}]$ q_0

i_0 $[1, n]$

n ξ_1 ξ_n $h_i = Y g^{\xi_i} \bmod p$

P_i g h_i $\mathcal{A}$

$\mathcal{R}$ $\mathcal{R}^\star$ $\mathcal{R}^\star$

$\mathcal{R}_j$ P_j

$\mathcal{R}_{i_0} = \mathcal{R}$ $\mathcal{R}_j = \mathcal{R}^\star$ $j \neq i_0$

$\mathcal{S}$

$\mathsf{Send}(U_j, \mathtt{start})$

a_j n $r_j, (b_{j,k})_{1 \leq k \leq n-1}$

$\mathcal{R}_j$ $j = i_0$

$q = q_0$ $n-1$ ρ_j

$j = 1, \ldots, n$ $j \neq i_0$ $A_{i_0,j} = X g^{\rho_j}$ $B_{i_0,j} = Z Y^{\rho_j} X^{\xi_j} g^{\rho_j \xi_j} a_{i_0}$

a_{i_0} $n-1$

U_j $n-1$

$n-1$

$a_{(j)}$ a_i $\mathcal{S}$

$x_j = \log_g h_j$

f_j

Reveal

U_{i_0} q_0 $\mathcal{S}$

Test q_0

$(\mathcal{Q}-1)/\mathcal{Q}$

$\kappa = a \cdot g^r = \prod_{i=1}^n a_i \cdot g^{\sum_{i=1}^n r_i}$ Test

β $\kappa_0 \leftarrow \mathcal{K}, \kappa_1 = \kappa$ $\mathcal{K}$

$\mathcal{K} = Q$ κ_β

b'

Claim 1 *If the simulator's input is a Diffie-Hellman triplet (that is $b = 1$) the adversary's view is perfectly indistinguishable from the real protocol.*

P_i a_i κ

sk

$sk = \kappa$

P_j $y + \xi_j$ $y = \log_g Y$ $C_{i_0,j}$

a_{i_0} $x + \rho_j$ $x = \log_g X$

$C_{i,j}$ a_i h_j

$\mathcal{A}_{\mathcal{V}}$

$$\begin{aligned}\Pr\left[\mathcal{A}_{\mathcal{V}}(\kappa_\beta) = 1 | \beta = 1 \wedge b = 1\right] &= \Pr\left[\mathcal{A}_{\mathcal{V}}(\kappa_\beta) = 1 \,\middle|\, \beta = 1 \wedge \kappa_1 = sk\right] \\ &= \Pr\left[\mathcal{A}_{\mathcal{V}}(\kappa_1) = 1 \,\middle|\, \kappa_1 = sk\right] \\ \Pr[\mathcal{A}_{\mathcal{V}}(\kappa_\beta) = 1 | \beta = 0 \wedge b = 1] &= \Pr\left[\mathcal{A}_{\mathcal{V}}(\kappa_\beta) = 1 \,\middle|\, \beta = 0 \wedge \kappa_0 \leftarrow \mathcal{K}\right] \\ &= \Pr\left[\mathcal{A}_{\mathcal{V}}(\kappa_0) = 1 \,\middle|\, \kappa_0 \leftarrow \mathcal{K}\right]\end{aligned}$$

$$\Pr[\beta = 1] = \Pr[\beta = 0] = 1/2$$

$$\Pr\left[\mathcal{A}_{\mathcal{V}}(\kappa_\beta) = 1 | b = 1\right] = \frac{1}{2}\Pr\left[\mathcal{A}_{\mathcal{V}}(\kappa_1) = 1 | \kappa_1 = sk\right] + \frac{1}{2}\Pr\left[\mathcal{A}_{\mathcal{V}}(\kappa_0) = 1 | \kappa_0 \leftarrow \mathcal{K}\right]$$

Claim 2 *If the simulator's input is a random triplet (that is $b = 0$) the adversary's view is independent from a_{i_0}.*

$C_{i_0,j}$ $C_{i_0,j}$

$h_j = Y g^{\xi_j}$

$$\hat{a}_{i_0,j} = \frac{B_{i_0,j}}{(A_{i_0,j})^{y+\xi_j}} = \frac{ZY^{\rho_j}X^{\xi_j}g^{\rho_j\xi_j}a_{i_0}}{(Xg^{\rho_j})^{y+\xi_j}} = \frac{g^{z+y\rho_j+x\xi_j+\rho_j\xi_j}a_{i_0}}{(g^{x+\rho_j})^{y+\xi_j}} = g^{z-xy}a_{i_0}$$

$z = \log_g Z$ j

additive

j $\hat{a}_{(j)} = g^{z-xy}\prod_k a_k = g^{z-xy}a_{(j)}$

$a_{(j)}$

sk

$$\hat{a} \cdot g^{\sum_{j=1}^{n} r_j} = g^{z-xy}a \cdot g^r.$$

$a_{(j)}$

P_i P_{i_0}

$\kappa_1 = ag^r$ a_{i_0} κ_1 Q κ_0

β $\mathcal{A}$

$$\Pr\left[\mathcal{A}_{\mathcal{V}}(\kappa_\beta) = 1 | b = 0\right] = \frac{1}{2}\Pr\left[\mathcal{A}_{\mathcal{V}}(\kappa_1) = 1 | \kappa_1 \leftarrow \mathcal{K}\right] + \frac{1}{2}\Pr\left[\mathcal{A}_{\mathcal{V}}(\kappa_0) = 1 | \kappa_0 \leftarrow \mathcal{K}\right]$$

$$
\begin{aligned}
\mathsf{Adv}^{\mathsf{ddh}}(\mathcal{S}) &= \Pr\left[b' = 1 | b = 1\right] - \Pr\left[b' = 1 | b = 0\right] \\
&= \Pr\left[\mathcal{A}_{\mathcal{V}}(\kappa_\beta) = 1 | b = 1\right] - \Pr\left[\mathcal{A}_{\mathcal{V}}(\kappa_\beta) = 1 | b = 0\right] \\
&= \frac{1}{2}\left(\Pr\left[\mathcal{A}_{\mathcal{V}}(\kappa_1) = 1 \middle| \kappa_1 = sk\right] - \Pr\left[\mathcal{A}_{\mathcal{V}}(\kappa_1) = 1 \middle| \kappa_1 \leftarrow \mathcal{K}\right]\right) + \frac{1}{2} \times 0 \\
&= \frac{\mathsf{Adv}(\mathcal{A})}{2}
\end{aligned}
$$

Test

$1/\mathcal{Q}$

Contributory –

a_i

r

5 Comments, Optimizations and Variants

Efficiency of the protocol –

$3|p|n$ $n+2$

$2n$

n

Considering forward-secrecy – ? ?

x_i x_i

x_1

$\mathcal{A}$ x_1 P_1

$a_2, \ldots, a_n$ P_1 a_1 $h_1 = g^{x_1}$

$\mathcal{A}$

?

Resistance to known-key attacks –

A General Solution –

6 Conclusions

Acknowledgments.

References

1. G. Ateniese, M. Steiner and G. Tsudik. New multi-party authentication services and key agreement protocols. *IEEE Selected Areas in Communications*, **18**(4): 628–639, 2000.
2. M. Bellare, R. Canetti and H. Krawczyk. A modular approach to the design and analysis of authentication and key exchange protocols. In *STOC '98*, pp. 419–428, 1998.
3. M. Bellare, D. Pointcheval and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In *Eurocrypt '00*, *LNCS* 1807, pp. 139–155. Springer, 2000.
4. M. Bellare and P. Rogaway. Random oracles are practical: a paradigm for designing efficient protocols. In *ACM CCS '93*, pp. 62–73. 1993.
5. M. Bellare and P. Rogaway. Entity authentication and key distribution. In *Crypto '93*, *LNCS* 773, pp. 232–249. Springer, 1993.
6. M. Bellare and P. Rogaway. Provably secure session key distribution: The three party case. In *STOC '95*, pp. 57–66, 1995.

7. S. Blake-Wilson, D. Johnson and A. Menezes. Key agreement protocols and their security analysis. In *Conf. on Cryptography and Coding*, *LNCS* 1355, pp. 30–45. Springer, 1997.
8. S. Blake-Wilson and A. Menezes. Authenticated Diffie-Hellman key agreement protocols. In *SAC '98*, *LNCS* 1556, pp. 339–361. Springer, 1998.
9. E. Bresson, O. Chevassut and D. Pointcheval. Provably authenticated group Diffie-Hellman key exchange – the dynamic case. In *Asiacrypt '01*, *LNCS*, pp. 290–309.
10. E. Bresson, O. Chevassut and D. Pointcheval. Dynamic group Diffie-Hellman key exchange under standard assumptions. In *Eurocrypt '02*, *LNCS* 2332, pp. 321–336.
11. E. Bresson, O. Chevassut and D. Pointcheval. The group Diffie-Hellman problems. In *SAC '02*, LNCS 2595, pp. 325–338. Springer, 2002.
12. M. Burmester and Y. G. Desmedt. A secure and efficient conference key distribution system. In *Eurocrypt '94*, *LNCS* 950, pp. 275–286. Springer, 1995.
13. C. Cachin, K. Kursawe, F. Petzold, and V. Shoup. Secure and efficient asynchronous broadcast protocols. In *Crypto '01*, *LNCS* 2139, pp. 524–541. Springer, 2001.
14. R. Canetti, S. Halevi and J. Katz. A forward-secure public-key encryption scheme. In *Eurocrypt '2003*, *LNCS* 2656, pp. 255–271, Springer, 2003.
15. R. Cramer V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *Crypto '98*, *LNCS* 1462, pp. 13–25. Springer.
16. W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, vol. 22(6): pp. 644–654, November 1976.
17. W. Diffie, P. van Oorschot and W. Wiener. Authentication and authenticated key exchange. In *Designs, Codes and Cryptography*, vol. 2(2), pp. 107–125, June 1992.
18. W. Diffie, D. Steer, L. Strawczynski and M. Wiener. A secure audio teleconference system. In *Crypto '88*, *LNCS* 403, pp. 520–528. Springer, 1988.
19. R. Dupont and A. Enge. Practical non-interactive key distribution based on pairings. Cryptology eprint archive, `http://eprint.iacr.org`, May 2002.
20. T. ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE IT*-31(4):469–472, 1985.
21. O.Goldreich, S. Goldwasser and S. Micali. How to Construct Random Functions. *JACM* **33**(4):792-807, 1986.
22. S. Goldwasser and S. Micali. Probabilistic Encryption. *JCSS*, 28(2):270–299, April 1984.
23. I. Ingemarsson, D. T. Tang and C. K. Wong. A conference key distribution system. *IEEE Transactions on Information Theory*, vol. IT-28(5): pp. 714–720, September 1982.
24. A. Joux. A one-round protocol for tripartite Diffie-Hellman. In *Proc. of ANTS-4 Conference*, vol. 1838 of *LNCS*, pp. 385–394, Springer-Verlag, 2000.
25. J. Katz and M. Yung. A fully scalable Protocol for Authenticated Group Key Exchange. In *Crypto '03*, to appear.
26. C.-H. Li and J. Pieprzyk. Conference key agreement from secret sharing. In *Proc. of ACISP '99*, vol. 1587 of *LNCS*, pages 64–76. Springer-Verlag, 1999.
27. D. Malkhi, M. Merrit and O. Rodeh. Secure Reliable Multicast Protocols in a WAN. In *Proc. of International Conference on Distributed Computing Systems*, pp. 87–94, 1997.
28. D. Malkhi and M. Reiter. A High-Throughput Secure Reliable Multicast Protocol. *J. of Computer Security*, vol. 5, pp. 113-127, 1997.
29. A. J. Menezes, P. V. Oorschot and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997. `http://cacr.math.uwaterloo.ca/hac/`.
30. A. Shamir. How to share a secret. In *CACM*, **22**:612–613. November 1979.
31. V. Shoup. On formal models for secure key exchange. Tech. Rep. RZ 3120, IBM Zürich Research Lab, November 1999.
32. M. Steiner, G. Tsudik and M. Waidner. Key agreement in dynamic peer group. *IEEE Transactions on Parallel and Distributed Systems*, vol. 11(8): pp. 769–780, August 2000.