A New Key Agreement Scheme Based On A Well-Known Property Of Powers

Michele Fabbrini
Mathematics Department, University of Pisa
email: 13518203@studenti.unipi.it
orcid: https://orcid.org/0000-0002-8870-8892

April 10, 2021

Abstract

In this paper I propose a new key agreement scheme applying a well-known property of powers to a particular couple of elements of the cyclic group generated by a primitive root of a prime p. The model, whose security relies on the difficulty of computing discrete logarithms when p is a "safe prime", consists of a five-step process providing explicit key authentication.

Keywords— public-key cryptography, key agreement scheme, discrete logarithm problem, implicit key authentication, explicit key authentication

Contents

1 Introduction **2**

2 The property **2**

3 The core of the model **2**

4 A new key agreement scheme proposal **2**
4.1 Step 1: Alice creates her secret and sends it to Bob 3
4.2 Step 2: Bob retrieves Alice's secret and sends her a confirmation 3
4.3 Step 3: Bob creates his secret and sends it to Alice 3
4.4 Step 4: Alice retrieves Bob's secret and sends him a confirmation 4
4.5 Step 5: The K-sequence is assembled 4

5 Authentication **4**
5.1 Implicit key authentication 4
5.2 Key confirmation 4
5.3 Explicit key authentication 4

6 Security **5**
6.1 Direct attack to the secrets 5
6.2 Man-in-the-middle attack 5

7 A very simple example **5**

8 Conclusions **6**

1 Introduction

As every element of a cyclic group is a power of a common base, the *"product of powers property"* can be applied to the multiplication among them. Based on this, I have developed a public-key cryptography model to allow the creation and secure exchange of the two halves of a secret key over an insecure channel. The scheme is conceived as a process where each party equally contributes to a sequence of bits able to be used as symmetric key for encryption and decryption of messages.

2 The property

The *"product of powers property"* states that when you multiply two powers with the same base, you keep the base and add the exponents

$$x^m * x^n = x^{m+n}$$

3 The core of the model

Let

- p be a prime
- $\phi_{(p)} = p - 1$ its totient
- g one of its primitive roots
- $\langle g \rangle$ the cyclic group generated by g
- g^h, g^k two generic elements of $\langle g \rangle$

Then consider the couple

$$g^{\phi_{(p)}},\ g^k$$

as a consequence of the above described property

$$g^{\phi_{(p)}} = g^k * g^{\phi_{(p)}-k}$$

multiplying both sides of the equality by g^h (and since $g^{\phi_{(p)}} = 1$)

$$g^h = g^h * g^k * g^{\phi_{(p)}-k}$$

This represents the core of the scheme. It says that *multiplying the element g^h by the element g^k, it is possible to recover g^h if one knows $\phi_{(p)}$ and k.*

4 A new key agreement scheme proposal

Alice and Bob share:

- a prime p and consequently its totient $\phi_{(p)} = p - 1$
- g a primitive root of p
- a K_{lenght} in bits

Bob and Alice agree to set up a $K - sequence$ of the shared K_{lenght} composed of two halves combined together. A five-step process starts where:

- steps 1-2 produce the first half-key
- steps 3-4 produce the second half-key
- in step 5 the two halves are combined together to produce a $K - sequence$ of the desired lenght

4.1 Step 1: Alice creates her secret and sends it to Bob

Bob generates

- a random key rb_1, a public key $B = g^{rb_1} \bmod p$

Alice generates

- a random key ra_1, a public key $A = g^{ra_1} \bmod p$
- a random key ra_2, a secret key $sa = g^{ra_2} \bmod p$, paying attention that

$$sa_{lenght} \geq \frac{K_{lenght}}{2}$$

  otherwise she tries a different ra_2
- a challenge $CHa = (sa * B) \bmod p$ and sends it to Bob. The challenge implies the question: "What is my secret?"

4.2 Step 2: Bob retrieves Alice's secret and sends her a confirmation

Bob calculates sa' using $\phi_{(p)}$ and rb_1

- $sa' = [CHa * (g^{\phi_{(p)} - rb_1} \bmod p)] \bmod p$

and sends a confirmation to Alice, multiplying sa' by Alice's public key

- $COb = (sa' * A) \bmod p$

Alice verifies Bob's confirmation calculating

- $Va = (sa * A) \bmod p$

and then comparing Va with COb

- $Va = COb$ means that $sa = sa'$. Consequently, Alice is assured that Bob has correctly received sa and is able to use it

4.3 Step 3: Bob creates his secret and sends it to Alice

Bob generates

- a random key rb_2, a secret key $sb = g^{rb_2} \bmod p$, paying attention that
$$sb_{lenght} \geq \frac{K_{lenght}}{2}$$
otherwise he tries a different rb_2
- a challenge $CHb = (sb * A) \bmod p$ and sends it to Alice. The challenge implies the question: "What is my secret?"

4.4 Step 4: Alice retrieves Bob's secret and sends him a confirmation

Alice calculates sb' using $\phi_{(p)}$ and ra_1

- $sb' = [CHb * (g^{\phi_{(p)} - ra_1} \bmod p)] \bmod p$

and sends a confirmation to Bob, multiplying sb' by Bob's public key

- $COa = (sb' * B) \bmod p$

Bob verifies Alice's confirmation calculating

- $Vb = (sb * B) \bmod p$

and then comparing Vb with COa

- $Vb = COa$ means that $sb = sb'$. Consequently, Bob is assured that Alice has correctly received sb and is able to use it

4.5 Step 5: The K-sequence is assembled

- Alice and Bob take the first $\frac{K_{lenght}}{2}$ bits of $sa = sa'$: this is the left part of the $K - sequence$
- Alice and Bob take the last $\frac{K_{lenght}}{2}$ bits of $sb' = sb$: this is the right part of the $K - sequence$

5 Authentication

5.1 Implicit key authentication

- At the end of step 1 Alice is certain that no one else except Bob can know her secret
- At the end of step 3 Bob is certain that no one else except Alice can know his secret

5.2 Key confirmation

- At the end of step 2 Alice is certain that Bob has correctly received her secret and can use it
- At the end of step 4 Bob is certain that Alice has correctly received his secret and can use it

5.3 Explicit key authentication

- At the end of step 4 both Alice and Bob hold implicit key authentication and confirmation

6 Security

6.1 Direct attack to the secrets

The here described model bases its security on the capacity to keep secret the four random keys. It would be possible for an attacker to find out the value of one or more of them, excluding chance, only if able to solve the discrete logarithm problem. Therefore, all the indications of the research findings regarding the choice of g and p emerged since the publication of the Diffie-Hellman [1] milestone work are valid. In particular:

- g should be a primitive root of p, so that the generated cyclic group $\langle g \rangle$ will have the largest order, i.e. $p-1$. On the other hand, a small g does not facilitate the calculation of the discrete logarithm, due to the Random Self-Reducibility [2], and therefore it can be chosen, for example, $g = 2$
- p must be large and such that $p-1$ contains a large prime factor to preclude feasibility of the discrete logarithm algorithm of Pohlig and Hellman [3], [4]
- p should be a *"safe prime"*, i.e. it should have the form $p = 2q + 1$, where q is a *Sophie Germain* prime [5]

6.2 Man-in-the-middle attack

- Since the scheme provides explicit key authentication, this type of attack is not effective

7 A very simple example

Let

- $p = 701$ and consequently $\phi_{(p)} = 700$
- $g = 2$
- $K_{lenght} = 16$ bits

Step 1

- $rb_1 = 10$, $B = 323$

- $ra_1 = 17$, $A = 686$
- $ra_2 = 52$, $sa = 260$, 9 bits $>$ 8 bits
- $CHa = 561$

Step 2

- $sa' = [561 * (2^{700-10} \bmod 701)] \bmod 701 = 260$
- $COb = (260 * 686) \bmod 701 = 306$
- $Va = 306 = COb$

Step 3

- $rb_2 = 33$, $sb = 463$, 9 bits $>$ 8 bits
- $CHb = (463 * 686) \bmod 701 = 65$

Step 4

- $sb' = [65 * (2^{700-17} \bmod 701)] \bmod 701 = 463$
- $COa = (463 * 323) \bmod 701 = 236$
- $Vb = 236 = COa$

Step 5

- 10000010 is the left part of the $K - sequence$
- 11001111 is the right part of the $K - sequence$
- $K - sequence$: 1000001011001111

8 Conclusions

In this work I describe a new *contributory* [6] key agreement scheme where an original use of a well-known property of powers produces, in a five-step process, a key of the desired length while providing explicit key authentication. The peculiarity of the proposed model is its simplicity which, together with the other characteristics illustrated in this paper, make it an ideal candidate for the development of a new class of protocols.

References

[1] W. Diffie and M. Hellman, *"New directions in cryptography,"* in IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, November 1976, doi: 10.1109/TIT.1976.1055638.

[2] J. Feigenbaum and L. Fortnow, *"On the random-self-reducibility of complete sets,"* [1991] Proceedings of the Sixth Annual Structure in Complexity Theory Conference, Chicago, IL, USA, 1991, pp. 124-132, doi: 10.1109/SCT.1991.160252.

[3] K.S. McCurley, *"The discrete logarithm problem"*, pp.49–74 in: Cryptology and Computational Number Theory — Proc. Symp. Applied Math., vol. 42 (1990). AMS.

[4] Oorschot, P. V. and Michael J. Wiener. *"On Diffie-Hellman Key Agreement with Short Exponents."* EUROCRYPT (1996).

[5] Kenichi Arai, and Hiroyuki Okazaki. *"Properties of Primes and Multiplicative Group of a Field."* Formalized Mathematics 17.2 (2009): 151-155.

[6] G. Ateniese, M. Steiner and G. Tsudik, *"New multiparty authentication services and key agreement protocols,"* in IEEE Journal on Selected Areas in Communications, vol. 18, no. 4, pp. 628-639, April 2000, doi: 10.1109/49.83993