Breaking and repairing a convertible undeniable signature scheme[1]

Markus Michels · Holger Petersen · Patrick Horster

Theoretical Computer Science and Information Security,
University of Technology Chemnitz-Zwickau,
Straße der Nationen 62, D-09111 Chemnitz, Germany
E-mail: {mmi,hpe,pho}@informatik.tu-chemnitz.de

Abstract

In 1990 Boyar, Chaum, Damgard and Pedersen introduced the concept of convertible, undeniable signatures. They proved that those schemes exist iff one-way functions exist and further gave an example of a practical convertible undeniable scheme which is based on the ElGamal signature scheme.

In this paper we present an attack on this signature scheme. After the conversion, that means, the signer releases the secret parameter so that his signature can be checked by any verifier, we can show that there is no security at all: A key only-attacker can forge the signature scheme universally. Thus this scheme might still be used as an undeniable signature scheme but it possesses only selective but no total convertibility. The attack can also be applied to Pedersen's modification of that scheme. We further show how the convertible, undeniable signature scheme can be repaired so that the attack doesn't fails and discuss a possibility to strengthen the security of the scheme.

1 Introduction

A property of conventional digital signature schemes [6] is that once a signature is released by the signer everybody can check its validity. There are situations where this property is not desirable. Here the signer should be able to determine which verifier should be able to verify a special signature and without limiting the set of possible verifiers.

In 1989 Chaum and van Antwerpen [4] suggested the notation of *undeniable* signature schemes which are characterized by the following properties.

1. The signer can decide freely (at any time) to whom he wants to prove the validity of his signature on a document.
2. The signer can prove that a wrong signature is not valid (disavowal protocol).
3. The signer can prove that a valid signature is indeed valid (confirmation protocol).
4. The signer can't prove that a valid signature is not valid.
5. The signer can't prove that an invalid signature is valid.

As a result, the signer can't deny signatures he has issued before. Chaum and van Antwerpen proposed the first undeniable signature scheme, later Chaum presented another scheme with zero-knowledge confirmation and disavowal protocols [2, 4].

However, a disadvantage of the scheme given in [4] is that several verifiers not trusting each other are able to verify a signature simultaneously. This attack was proposed by Desmedt and Yung [5], criticized by Chaum [3] and later strengthened by Jakobsson [11]. Furthermore, Jakobsson pointed out that in the protocol given in [4] the prover never knows what signature is being verified. This can be used by a blackmailer to show the validity of a signed, compromising message to the signer's enemies if the signer agrees to prove the validity of an innocent signed message [11]. However, there are ways to overcome these weaknesses. By proving that either the signature is valid or the prover is the chosen verifier, it's impossible for this verifier to convince other verifiers later, this mechanism is called designated verifier proof (see [12] for details).

Additionally, modified concepts were presented: Fujioka, Okamoto and Ohta suggested to combine the disavowal and confirmation protocol [8] and Boyar, Chaum, Damgard and Pedersen proposed the concept of (selectively) convertible undeniable signatures [1]. In the later concept undeniable signature schemes can be converted into conventional signature schemes for all messages or (in the selective case) only for chosen

[1] appeared in Proc. of 3rd ACM Conference on Computers and Communications Security, New Delhi, ACM Press, (1996), pp. 148 – 152.

signatures. They proved that secure convertible undeniable signature schemes exist if one-way functions do. Furthermore, they presented an ElGamal-like (selectively) convertible undeniable signature scheme.

In this paper we review this ElGamal-like selectively convertible undeniable signature scheme, show how to break this signature scheme after it is converted for all messages and how to repair it. Furthermore, we discuss how to strengthen the security of the repaired scheme.

2 An ElGamal-like convertible signature scheme

Now we briefly review the signature scheme described in [1].

Initialization
The certification authority chooses large primes p, q with $q|(p-1)$ and a generator α with order q. These parameters are common to all users.

Key generation
Each user generates secret parameters $x, z \in \mathbf{Z}_q^*$ and computes $y := \alpha^x \pmod p$. Furthermore, he calculates $u := \alpha^z \pmod p$. His secret keys are (x, z) and his corresponding public keys are (y, u).

Signature generation
To sign a message m, a signer picks random $t, k \in \mathbf{Z}_q^*$ and computes $T := \alpha^t \pmod p$ and $r := \alpha^k \pmod p$. He solves the signature equation

$$T \cdot t \cdot h(m) \cdot z \equiv x \cdot r + k \cdot s \pmod q$$

for the parameter s using the (collision free) public hash function h. The triple (T, r, s) is the signature on the message m.

Confirmation protocol
The signer can convince any verifier of his choice of the validity of a signature. As the verification equation

$$(T^{Th(m)})^z \equiv y^r \cdot r^s \pmod p \qquad (1)$$

holds if a signature is valid, the signer can prove that the discrete logarithm of $y^r \cdot r^s \pmod p$ to the base $T^{Th(m)} \pmod p$ is the same as the discrete logarithm of u to the base α using the zero-knowledge protocol of the equality of two discrete logarithms due to Chaum [2]. Clearly, it is assumed that proving the equality of two discrete logarithms can't be done without the help of the signer.

Disavowal protocol
The signer can convince any verifier of his choice of the invalidity of a wrong signature. As the verification equation

$$(T^{Th(m)})^z \equiv y^r \cdot r^s \pmod p$$

does not hold if a signature is invalid, the signer can prove that the discrete logarithm of $y^r \cdot r^s \pmod p$ to base $T^{Th(m)} \pmod p$ is different to the discrete logarithm of u to base α using the zero-knowledge protocol of the inequality of two discrete logarithms due to Chaum [2]. Here it is assumed that proving the inequality of two discrete logarithms can't be done without the help of the signer.

Selective conversion
By releasing the secret value t, exactly the signature which uses t can be checked by any verifier using the equations

$$u^{t \cdot T \cdot h(m)} \equiv y^r \cdot r^s \pmod p$$

and

$$T \equiv \alpha^t \pmod p.$$

Total conversion
By releasing the secret parameter z, every signature can be checked by any verifier by equation (1). Clearly, the authenticity of z can be checked by

$$u \equiv \alpha^z \pmod p.$$

3 Breaking the totally converted scheme

We demonstrate how the signature scheme can be forged universally if the secret parameter z is released. Then, the underlying conventional signature scheme is insecure. The task of an attacker is to find (T, r, s) for a given message m, such that

$$(T^{T \cdot h(m)})^z \equiv y^r \cdot r^s \pmod p.$$

As he knows z and y, he picks a random $a \in \mathbf{Z}_q^*$ and computes $r := y^a \pmod p$ and $T := r^d \pmod p$ using an arbitrary integer $d \in \mathbf{Z}_q^*$. Then the verification equation (1) is transformed to

$$r \equiv y^{r \cdot (T \cdot d \cdot h(m) \cdot z - s)^{-1}} \pmod p.$$

Therefore $a \equiv r \cdot (T \cdot d \cdot h(m) \cdot z - s)^{-1} \pmod q$. This equation can be solved for parameter s by

$$s := T \cdot d \cdot h(m) \cdot z - a^{-1} \cdot r \pmod q.$$

As a result, (T, r, s) is a signature on the message m, because

$$(T^{T \cdot h(m)})^z \equiv r^{d \cdot T \cdot h(m) \cdot z} \equiv$$

$$y^{a \cdot d \cdot T \cdot h(m) \cdot z} \equiv y^{a \cdot (s + a^{-1} \cdot r)} \equiv r^s \cdot y^r \pmod p.$$

Thus, the signature scheme might be used as a selectively convertible undeniable signature scheme but is not totally convertible into a conventional one.

Clearly, the same attack can be applied to Pedersen's modification of this scheme [14], *after* the scheme is totally converted by the signer. Again, if the conversion is only selectively done by distributing pieces of the parameter t to several agents (and this is the main contribution of that paper) the attack doesn't work and the scheme is still secure in this case.

4 Discussion

The design problem of the scheme described in section 2 after total conversion is the following: By choosing the parameter T in relation to r the scheme can be transformed into an insecure variant of the Meta-signature scheme, where one coefficient, more precisely coefficient A, is chosen equal to zero (see [10] for details). As a result, it is necessary that there are at least two authentically known parameters used as bases in the verification equation. In the conventional ElGamal-like signature schemes these are the generator and the public key of the signer. According to this fact, it is possible to countermeasure attacks similar to the one described in section 2 as we will show in the next section. Furthermore, an implication of the attack is that additional non-authentic parameters (here the parameter T) do not increase the security of a signature scheme, but might even weaken the system. Such a signature scheme based on the discrete logarithm can be regarded as a variant of a further extension of the Meta-signature scheme. However, it can always be reduced to a variant of the Meta-signature scheme by substituting every non-authentic parameter except r and s by a multiplicative combination of α, y and r, e.g. $T := \alpha^u \cdot y^v \cdot r^w \pmod p$ with suitable $u, v, w \in \mathbf{Z}_q^*$ different for each non-authentic parameter. The efficiency to generate or verify a signature with more authentic parameters is slightly decreased and the size of the signature is bigger. Thus adding an additional non-authentic parameter in such signature schemes can only be recommended in those concepts in which additional properties can be gained by these additional parameters.

5 How to repair the scheme using heuristic methods

The scheme described in section two can be repaired in a heuristic way such that the attack described above is prevented. Clearly, as in all ElGamal-like scheme the security can't be proven. The protocols for initialization, key generation, total conversion and selective conversion are the same as before, while the protocol for signature generation, the confirmation and disavowal protocol are modified in the following way:

Signature generation
To sign a message m, a signer chooses $t, k \in \mathbf{Z}_q^*$ at random and computes $T := \alpha^t \pmod p$ and $r := \alpha^k \pmod p$. He solves the signature equation

$$T \cdot t \cdot h(m) \cdot z \equiv x \cdot r + k \cdot s + 1 \pmod q$$

for the parameter s using the (collision free) public hash function h. Then (T, r, s) is the signature on the message m.

Confirmation protocol
The signer can convince any verifier of his choice of the validity of a signature. As the verification equation

$$(T^{T \cdot h(m)})^z \equiv y^r \cdot r^s \cdot \alpha \pmod p$$

holds if a signature is valid, the signer can prove that the discrete logarithm of $y^r \cdot r^s \cdot \alpha \pmod p$ to the base $T^{T \cdot h(m)} \pmod p$ is the same as the discrete logarithm of u to the base α using a zero-knowledge protocol of the equality of two discrete logarithms.

Disavowal protocol
The signer can convince any verifier of his choice of the invalidity of an invalid signature. As the verification equation

$$(T^{T h(m)})^z \equiv y^r \cdot r^s \cdot \alpha \pmod p$$

does not hold if a signature is invalid, the signer can prove that the discrete logarithm of $y^r \cdot r^s \cdot \alpha \pmod p$ to the base $T^{T h(m)} \pmod p$ is different to the discrete logarithm of u to the base α using a zero-knowledge protocol of the inequality of two discrete logarithms.

6 Security considerations

We argue that even a more generalized attack described above doesn't work any more: Again, the task of an attacker is to find (T, r, s) for a given message m, so that

$$(T^{T h(m)})^z \equiv y^r \cdot r^s \cdot \alpha \pmod p.$$

holds. As he knows z and y, he can fix r and T by

$$r := y^a \cdot \alpha^b \pmod p$$

and

$$T := y^c \cdot \alpha^d \pmod p$$

with some $a, b, c, d \in \mathbf{Z}_q^*$.

With $f := T \cdot h(m) \cdot z \pmod q$ the verification equation can be transformed to

$$y^{-r+c\cdot f-a\cdot s} \equiv \alpha^{1-d\cdot f+b\cdot s} \pmod p$$

We assume that the exponents on both sides of this equation are equal to 0 modulo q to fulfil the equation (any non-trivial exponents known to the attacker would enable him to compute the secret key). Therefore we get

$$-r + c \cdot f - a \cdot s \equiv 0 \pmod p$$

and

$$1 - d \cdot f + b \cdot s \equiv 0 \pmod p.$$

By eliminating the parameter s we obtain

$$a + b \cdot r \equiv (a \cdot d + b \cdot c) \cdot f \pmod q. \qquad (2)$$

As it's not known how to choose a, b and r (c, d and T) simultaneously, the goal of the attacker is to eliminate r and T from the equation (2). Note that neither a, b nor c, d should be 0 both, because otherwise r or T are equal to 1. The attack of section 3 can be transformed to such an attack. Here the attacker chooses $b = 0$ to eliminate r and $ad = -bc$ to eliminate T which determines f. As $a \neq 0$ must hold, we have $d = 0$. Now the equation (2) simplifies to $a = 0$ which is a contradiction.

Clearly, nothing can be proved here, but it should be noted that e.g. the security of the DSA [13] relies on a similar problem, which is sufficient (but not neccessary) to forge a DSA-signature universally : If $r := (\alpha^a \cdot y^b \pmod p) \pmod q$ for a given m and the attacker is able to find a, b, r such that

$$r \equiv a^{-1} \cdot b \cdot h(m) \pmod q,$$

holds, he could compute $s := h(m) \cdot a^{-1} \pmod q$. As a result, the congruence

$$r \equiv (\alpha^{h(m)\cdot s^{-1}} \cdot y^{r\cdot s^{-1}} \pmod p) \pmod q$$

would hold. Therefore he could find a DSA-signature (r, s) for the message m.

7 How to strengthen the security of the repaired scheme

The security of the repaired scheme can be strengthend in the case where the signer is honest. Let the signer additionally prove in zero-knowledge in the confirmation protocol that he knows the discrete logarithms of the parameters r and T using the protocol given in [15]. If the signer proves the validity of a valid signature and the verifier accepts the proof then the verifier knows that the signer knows the parameter k, t and z and therefore the secret key x. If an attacker has forged a signature for a (even non-sencial) message *and* can convince the verifier in the confirmation protocol that this signature is valid then the verifier knows that the attacker must know the secret keys x and z. Therefore existential forgery is equivalent to a total break of the scheme in this case. However, if the signer claims a signature to be wrong but can't prove it, it is not possible to prove anything about the attacker's knowledge or strength. Thus the security of the scheme is still heuristic. It would be desirable to obtain an efficient convertible undeniable signature scheme which is provably secure in the sense of Goldwasser, Micali and Rivest [9].

8 Conclusion

We have pointed out that the ElGamal-like convertible undeniable signature scheme proposed by Boyar, Chaum, Damgard and Pedersen is insecure if it is converted totally. We have further shown that the scheme can be repaired so that the attack doesn't work any more and discussed some ways to strengthen the security of the repaired scheme. However, the security of the modified scheme can't be proven and is only heuristic. Further work should be done to develop a provably secure, efficient convertible undeniable signature scheme.

9 Acknowledgement

The authors would like to thank Markus Jakobsson for helpful comments.

References

[1] J.Boyar, D.Chaum, I.Damgard, T.Pedersen, "Convertible undeniable signatures", Lecture Notes in Computer Science 537, Advances in Cryptology: Proc. Crypto '90, Springer Verlag, (1991), pp. 189–205.

[2] D.Chaum, "Zero-knowledge undeniable signatures", Lecture Notes in Computer Science 473, Advances in Cryptology: Proc. Eurocrypt '90, Springer Verlag, (1991), pp. 458–464.

[3] D.Chaum, "Some weakness of "Weaknesses of Undeniable Signatures"", Lecture Notes in Computer Science 547, Advances in Cryptology: Proc. Eurocrypt '91, Springer Verlag, (1992), pp. 554–556.

[4] D.Chaum, H. van Antwerpen, "Undeniable Signatures", Lecture Notes in Computer Science 435, Advances in Cryptology: Proc. Crypto '89, Springer Verlag, (1990), pp. 212–216.

[5] Y.Desmedt, M.Yung, "Weaknesses of undeniable signature schemes", Lecture Notes in Computer Science

547, Advances in Cryptology: Proc. Eurocrypt '91, Springer Verlag, (1992), pp. 205–220.

[6] W.Diffie, M.Hellmann, "New directions in cryptography", IEEE Transactions on Information Theory, Vol. IT-22, No. 6, November, (1976), pp. 644–654.

[7] T.ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, Vol. IT-30, No. 4, July, (1985), pp. 469 – 472.

[8] A.Fujioka, T.Okamoto, K.Ohta, "Interactive Bi-Proof Systems and undeniable signature schemes", Lecture Notes in Computer Science 547, Advances in Cryptology: Proc. Eurocrypt '91, Springer Verlag, (1992), pp. 243–256.

[9] S.Goldwasser, S.Micali, R.Rivest, "A digital signature scheme secure against adaptive chosen message attacks", SIAM Journal on Computing, Vol. 17, No. 2, (1988), pp. 281 – 308.

[10] P.Horster, M.Michels, H.Petersen, "Meta-ElGamal signature schemes", Proc. of the 2nd ACM Conference on Computer and Communication Security, Fairfax, (1994), pp. 96–107.

[11] M.Jakobsson, "Blackmailing using undeniable signatures", Lecture Notes in Computer Science 950, Advances in Cryptology: Proc. Eurocrypt'94, Springer Verlag, (1995), pp. 425–427.

[12] M.Jakobsson, "Designated verifier proofs or making proofs of knowledge non-transferable", manuscript, (1995), available at:
http://www-cse.ucsd.edu/users/markus

[13] National Institute of Standards and Technology, Federal Information Processing Standards, Publication, FIPS Pub 186, Digital Signature Standard (DSS), May 19, (1994), 20 pages.

[14] T.P.Pedersen, "Distributed provers with applications to undeniable signatures", Lecture Notes in Computer Science 547, Advances in Cryptology: Proc. Eurocrypt '91, Springer Verlag, (1992), pp. 221–242.

[15] C.P.Schnorr, "Efficient signature generation for smart cards", Journal of Cryptology, Vol. 4, (1991), pp. 161–174.