A Note on Signature Transformation Attacks and Confirmer Signatures

Victor K. Wei

Dept. of Information Engineering, The Chinese Univ. of Hong Kong, Hong Kong
kwwei@ie.cuhk.edu.hk

October 2, 2006

Abstract. Camenisch and Michels in Eurocrypt 2000 introduced the signature trnaformation attack on designated confirmer signatures (DCS). We apply this attack on Gentry, et al. Asiacrypt 2005's DCS, and on Goldwasser, et al. TCC 2004's DCS before repairing them. We also optimize efficiencies of the former DCS' confirmation and disavowal protocols. The undeniable signature of Laguillaumie, et al. in Indocrypt 2005 is upgraded using techniques above.

1 The results

Chaum [5] introduced the DCS (Designated Confirmer Signature). The signature verification requires the interaction with a confirmer who was designated by the signer when the signature was created. The motivation was to split the power to sign and the power to confirm in order to mitigate the overpower of the signer. Several applications benefit from such a power splitting [5, 1].

T. Okamoto [13] gave a formal security model for DCS, and a polynomial equivalence reduction between DCS and public-key encryption. Camenisch and Michels [4] presented an upgraded DCS security model which included the *signature transformation attacker* who can query the confirmation oracle with adaptively designed signer public key which is not obtained by the given key generation protocol. [4] also gave concrete instantiations, using the RSA signature and the Cramer-Shoup encryption. The confirmation and disavowalwere not very efficient as they involved double discrete logarithms or range proofs.

Goldwasser and Waisbard [10] and Gentry, et al. [9] presented DCS without random oracles. [9]'s DCS has $O(1)$-size and the state-of-the-art efficiency of costing 10 (resp. 41) exponentiations in confirm (resp. disavow).

The **contributions** of this note: We apply Camenisch and Michels [4]'s signature transformation attack on the two DCS's above, before repairing them. The attack on [9] is within their model while the attack on [10] is beyond their model. We also optimize the efficiencies of [9]'s confirmation and disavowal protocols. The undeniable signature of Laguillaumie, et al. [12] is upgraded using techniques above.

In this brief note, we do not include the security model or other definitions of terminologies. Consult the original references for details [4, 10, 9].

Attack and repair on Gentry, et al. [9]. In summary, the main DCS in [9] on message m is $\sigma' = (\sigma^*, \phi, c)$, where

$$\phi = Commit(m, r) = g^m h^r \in QR_{n^2} \tag{1}$$
$$c = \mathsf{Enc}(\mathsf{pk}_C, r) = (u_1, u_1, u_3, u_4) = (g_1^\rho, g_2^\rho, d_3^\rho g_0^r, (d_1 d_2^\alpha)^\rho) \in QR_{n^2}^4 \tag{2}$$
$$\sigma^* = \mathsf{Sign}(\mathsf{sk}_S, (\phi, c, \mathsf{pk}_S)) \tag{3}$$

where $\alpha = Hash(u_1,\ u_2,\ u_3)$. The commitment is Pedersen's commitment. The base $g_0 = n + 1$ allows the confirmer to compute the *partial discrete logarithm* in the Paillier system, and thus decrypt r. Sign is any secure signature without random oracles, with signer private key sk_S. The confirmer public key pk_C consists of $d_1 = g_1^{x_1} g_2^{x_2}$, $d_2 = g_1^{y_1} g_2^{y_2}$, $d_3 = g_1^z$. Its private key is $\mathsf{sk}_C = (x_1,\ x_2,\ y_1,\ y_2,\ z)$.

The *signature transformation attack*: Generate the transformed signature $\bar{\sigma}' = (\bar{\sigma}^*,\ \bar{\phi},\ \bar{c})$ on message $\bar{m} = m + 1$ by computing $\bar{c} = c$, $\bar{r} = r$, $\bar{\phi} = \phi g$, and computing $\bar{\sigma}^*$ using attacker's knowledge of sk_S which is granted in the security model. The transformed DCS has the same validity/invalidity as the pre-transformation DCS. Interacting with the confirmation oracle yields the validity/invalidity of the transformed DCS, and consequently the validity/invalidity of the original pre-transformation DCS. Therefore, an adversary $\mathcal{A}$ can distinguish a valid signture from an invalid one by interacting with the confirmation oracle, and thus breaking the security of the DCS. Note that replacing Equation (1) by $\phi = g^{H(m)} h^r$ is not a sufficient defense as we can use $\bar{\phi} = \phi g^{H(\bar{m}) - H(m)}$ and achieve the same attack.

Repair: Change α above to

$$\alpha = Hash(u_1, u_2, u_3, \phi, \mathsf{pk}_S, \mathsf{pk}_C, m)$$

When queried with anything other than the (DCS, pk_S, m), the confirmation oracle will not yield any non-negligible advantage on the invisibility of the validity the DCS [4].

Using the repair above, we can explicitly upgrade the part of [9]'s security model to the corresponding part in [4] that defends signature transformation attacks. Below, we also optimize [9]'s four-move concurrent zero-knowledge confirmation/disavowal protocols.

We omit the straightforward confirmation protocol $CZK\{r : \phi g^{-m} = h^r\}$. To disavow, prove either of the following:

$$CZK\{(x_1, x_2, y_1, y_2) : d_1 = g_1^{x_1} \wedge d_2 = g_1^{y_1} g_2^{y_2} \wedge u_4 \neq g_1^{x_1+\alpha y_1} g_2^{x_1+\alpha y_2}\}$$

$$CZK\{(z, \bar{r}) : d_3 = g_1^z \wedge u_3 = u_1^z g_0^{\bar{r}} \wedge \phi g^{-m} \neq h^{\bar{r}}\}$$

They are equivalent to, respectively,

$$CZK\{(x_1, x_2, y_1, y_2, s_0, s_1 = s_0 x_1, s_2 = s_0 y_1, s_3 = s_0 x_2, s_4 = s_0 y_2) : d_1 = g_1^{x_1} g_2^{x_2} \wedge d_2 = g_1^{y_1} g_2^{y_2} \wedge T = u_4^{-s_0} g_1^{s_1+\alpha s_2} g_2^{s_3+\alpha s_4} \wedge 1 = d_1^{s_0} g_1^{-s_1} g_2^{-s_3} \wedge 1 = d_2^{s_0} g_1^{-s_2} g_2^{-s_4}\} \text{ with } T \neq 1$$

$$CZK\{(z, \bar{r}, s_0, s_1 = s_0 \bar{r}) : d_3 = g_1^z \wedge u_3 = u_1^z g_0^{\bar{r}} \wedge T = (\phi^{-1} g^m)^{s_0} g^{s_1} \wedge T_4 = g_4^{s_0} \wedge 1 = T_4^{\bar{r}} g_4^{-s_1}\} \text{ with } T \neq 1$$

The confirmation costs 4 moves totalling 3 exponentiations. The disavow costs 4 moves totally at most 32 exponentiations. In comparison, [9]'s confirmation (resp. disavowal) costs 4 moves and 10 exponentiations (resp. 16 moves and 41 exponentiations). We demonstrate the second CZK:

1. Verfier select random c', sends $c'' = Hash(c')$.
2. Prover sends T, T_4, and $D_3 = g_1^{r_z}$, $D_u = u_1^{r_z} g_0^{r_r}$, $D_T = (\phi^{-1} g^m)^{r_0} g^{r_1}$, $D_4 = g_4^{r_0}$, $D_5 = T_4^{r_r} g_4^{-r_1}$.
3. Verifier checks $T \neq 1$ and sends c'.
4. Prover checks $c'' = Hash(c')$, sends $z_z = r_z - c'z$, $z_r = r_r - c'\bar{r}$, $z_0 = r_0 - c's_0$, $z_1 = r_1 - c's_1$.

Finally, Verifier checks the following before outputting 1: $D_3 = g_1^{z_z} d_3^{c'}$, $D_u = u_1^{z_z} g_0^{z_r} u_3^{c'}$, $D_T = (\phi^{-1} g^m)^{z_0} g^{z_1} T^{c'}$, $D_4 = g_4^{z_0} T_4^{c'}$, $D_5 = T_4^{z_r} g_4^{-z_1}$.

Attack generalization and repair: Other DCS schemes that use encryption as a black-box building block, such as those in [10, 9] and elsewhere, may also risk signature transformation attacks. Our results suggest these schemes may have an easy upgrade path by opening the black box slightly and add more parameters to the hash input or to the input of other kinds of *tag* generating mechanisms. We demonstrate a similar signature transformation attack on the DCS in [10] below.

Attack and repair on Goldwasser, et al. [10]. We focus on the first DCS in [10] which is based on the Cramer-Shoup signature [8] and the Cramer-Shoup encryption [7]. The Cramer-Shoup signature on message m is $\sigma' = (e, y', y)$,

$$y^e = xh^{H(x')}$$
$$x' = (y')^{e'} h^{-H(m)}$$

where the signer's public key is $\mathsf{pk}_S = (n,\, h,\, x,\, e')$, n is a product of two primes, e' and e' are distinct primes, h and x are random. The Goldwasser, et al.'s DCS is $\sigma = (\sigma_1 = e,\, \sigma_2 = y',\, \sigma_3 = \mathsf{Enc}(\mathsf{pk}_C,\, y)\ )$.

The *signature transformation attack*: Generate the transformed signature $\bar{\sigma} = (\bar{e},\, \bar{y}',\, \sigma_3)$ on a new message $\bar{m}$ for a new signer public key $\bar{\mathsf{pk}}_S = (n,\, \bar{h},\, \bar{x},\, e')$ where $\bar{x} = y^e$, $\bar{h} = y$, $\bar{x}' = (y')^{e'} \bar{h}^{-H(\bar{m})}$, $\bar{e} = e + H(\bar{x}')$. It is mechanical to verify that the transformed DCS has the same validity/invalidity as the pre-transformation DCS. Interacting with the confirmation oracle yields the validity/invalidity of the transformed DCS, and consequently the validity/invalidity of the original pre-transformation DCS. Note in verifying the signature, it is a common practice to not check e (resp. $\bar{e}$) is a prime, only to check that it is within a certain range [8, 10]. We use this practice in our attack hyphtheses.

Therefore, an adversary $\mathcal{A}$ can distinguish a valid signture from an invalid one by interacting with the confirmation oracle. However, [10] does not claim the indistinguishability between valid and invalid signatures, called the *invisibility of the signature* in [13, 4]. Our attack is beyond their security model. Their DCS remains secure in their own model. Nevertheless, we suggest to include more parameters in the has inputs wherever possible to defend against signature transformation and potentially other attacks. For example, letting $x' = (y')^{e'} h^{-H(m, \mathsf{pk}_S, e, y')}$ or having even more parameters included in the hash inputs can contribute to enhanced security.

Upgrading [12]'s undeniable signature to achieve signature invisibility. Undeniable signatures [6] are DCS's where signer and confirmer are the same entity. Using techniques developed above, we can modify Laguillaumie, et al. [12]'s undeniable signature without random oracles to upgraded security model with signature invisibility and defense against signature transformation attackers. Consult original references for details of the security model.

1. *Setup*. The signer public key $\mathsf{pk} = (n,\, y_1,\, y_2,\, {}_1,\, d_2,\, d_3)$, $\mathsf{sk} = (x_1,\, x_2,\, \bar{x}_1,\, \bar{x}_2,\, \bar{y}_1,\, \bar{y}_2,\, z)$, where $y_1 = g^{x_1}$, $y_2 = g^{x_2}$, $d_1 = g_1^{\bar{x}_1} g_2^{\bar{x}_2}$, $d_2 =$

$g_1^{\bar{y}_1} g_2^{\bar{y}_2}$, $d_3 = g_1^z$, n is a product of two safe primes p and q, pairings $\hat{\mathbf{e}} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$, order$(\mathbb{G}_1) = n$, $g \in \mathbb{G}_1$, g_1, $g_2 \in \mathbb{Z}_{n^2}$, $g_0 = n+1$.

2. *Sign.* Select random $R \in \mathbb{Z}_n$, compute $\sigma = (\sigma_1, \sigma_2)$, where $\sigma_1 = g^{1/(x_1+R+mx_2)}$, $\sigma_2 = \mathsf{Enc}(R) = (u_1, \cdots, u_4)$ with $u_1 = g_1^r$, $u_2 = g_2^r$, $u_3 = d_3^r g_0^R$, $u_4 = (d_1 d_2^\alpha)^r$, where $\alpha = Hash(u_1, u_2, u_3, m, \mathsf{pk}, \sigma_1)$.
3. *Confirm/disavow.* To confirm, prove the following concurrent zero-knwoledge protocols:

$$CZK\{R : \hat{\mathbf{e}}(\sigma_1, y_1 y_2^m)\hat{\mathbf{e}}(\sigma_1, g)^R = \hat{\mathbf{e}}(g, g) \ \wedge \ u_3 = u_1^z g_0^R \ \wedge \ d_3 = g_1^z\}$$

To disavow, prove the following concurrent zero-knwoledge protocol

$$\begin{aligned} &CZK\{(\bar{x}_1, \bar{x}_2, \bar{y}_1, \bar{y}_2, z, R') : d_1 = g_1^{\bar{x}_1} g_2^{\bar{x}_2} \\ &\quad \wedge \ d_2 = g_1^{\bar{y}_1} g_2^{\bar{y}_2} \ \wedge \ d_3 = g_1^z \ \wedge \ u_3 = u_1^z g_0^{R'} \\ &\quad \wedge \ [u_4 \neq u_1^{\bar{x}_1+\alpha\bar{y}_1} u_2^{\bar{x}_2+\alpha\bar{y}_2} \ \vee \ \hat{\mathbf{e}}(\sigma_1, y_1 y_2^m)\hat{\mathbf{e}}(\sigma_1, g)^{R'} \neq \hat{\mathbf{e}}(g, g)\} \end{aligned}$$

Note order$(g_0) = n$ in $\mathbb{Z}_{n^2}$. There is no need to prove for the *proof of range* that R (and R') lie in the interval $[0, n)$. Th invisibility of signature mainly follows the use of concurrent zero-knowledge protocols. The unforgeability of the undeniable signature can be proved similarly to [12]. Methods to instantiate a pairings group (or *gap Diffie-Hellman group*) $\mathbb{G}_1$ with a composite order n were described in Boneh, et al. [3] and Groth, et al. [11].

Generalization. The undeniable signature above combines Boneh, et al. [2]'s signature without random oracles and the famous Cramer-Shoup encryption [7] without random oracles. It can be modified into a DCS by separating the signing key (given to the signer) and the encryption key (given to the confirmer). But then the confirmer key, $\mathsf{pk}_C = (d_1, d_2, d_3)$, is dependent of the signer public key n, as the three entries lie in $\mathbb{Z}_{n^2}$. Although security is not compromised because the security of the Cramer-Shoup encryption reduces to the decisional Diffie-Hellman assumption in $\mathbb{Z}_{n^2}$ which continues to hold, this dependence is not desirable. If entries of pk_C are in $\mathbb{Z}_{\bar{n}^2}$ with $\bar{n} \neq n$, then inefficient range proofs may have to be used in the confirmation/disavowal protocol.

Acknowledgements to Hong Kong Earmarked Grants 4232-03E and 4328-02E for sponsorship.

References

1. N. Asokan, Victor Shoup, and Michael Waidner. Optimistic fair exchange of digital signatures. In *EUROCRYPT 1998*, pages 591–606, 1998.

2. D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *Proc. CRYPTO 2004*, pages 41–55. Springer-Verlag, 2004. Lecture Notes in Computer Science No. 3152.
3. Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-DNF formulas on ciphertexts. In *TCC 2005*, pages 325–341, 2005.
4. J. Camenisch and M. Michels. Confirmer signature schemes secure against adaptive adversaries. In *Eurocrypt 2000*, pages 243–258. Springer-Verlag, 2000. LNCS No. 2729.
5. D. Chaum. Designated confirmer signatures. In *Eurocrypt'94*, pages 86–91. Springer-Verlag, 1994. LNCS No. 435.
6. D. Chaum and H. van Antwerpen. Undeniable signatures. In *Crypto'89*, pages 286–299, 1989.
7. R. Cramer and V. Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 45–64. Springer-Verlag, 2002.
8. Ronald Cramer and Victor Shoup. Signature schemes based on the strong rsa assumption. *ACM Trans. Inf. Syst. Secur.*, 3(3):161–185, 2000.
9. Craig Gentry, David Molnar, and Zulfikar Ramzan. Efficient designated confirmer signatures without random oracles or general zero-knowledge proofs. In *ASIACRYPT 2005*, volume 3788 of *LNCS*, pages 662–681. Springer-Verlag, 2005.
10. Shafi Goldwasser and Erez Waisbard. Transformation of digital signature schemes into designated confirmer signature schemes. In *TCC 2004*, volume 2951 of *LNCS*, pages 77–100. Springer-Verlag, 2004.
11. Jens Groth, Rafail Ostrovsky, and Amit Sahai. Perfect non-interactive zero knowledge for NP. Cryptology ePrint Archive, Report 2005/290.
12. Fabien Laguillaumie and Damien Vergnaud. Short undeniable signatures without random oracles: The missing link. In *INDOCRYPT 2005*, volume 3797 of *LNCS*, pages 283–296. Springer-Verlag, 2005.
13. T. Okamoto. Designated confirmer signatures and public-key encryption are equivalen. In *Proc. CRYPTO '94*, pages 61–74, 1994.