A Strong Proxy Signature Scheme with Proxy Signer Privacy Protection

K. Shum and Victor K.Wei
Department of Information Engineering, Chinese University of Hong Kong, Hong Kong
Email: kshum0@ie.cuhk.edu.hk , kwwei@ie.cuhk.edu.hk

Abstract **--- Mambo, et al. [3] discussed the delegation of signature power to a proxy signer. Lee, et al. [5] constructed a strong non-designated proxy signature scheme in which the proxy signer had strong non-repudiation. In this paper, we present an enhancement to their scheme such that the identity of the proxy signer is hidden behind an alias. The identity can be revealed only by the alias authority. We also discuss other applications of this technique.**

I. Introduction

Delegating the power of signature to a proxy is useful in many scenarios. Traveling executives can delegate to their secretaries to sign certain documents during their absence. Managers can delegate to their subordinates to perform certain signature. Delegating the power of digital signature on digital documents to a proxy creates many technical challenges.

The idea of proxy signature was discussed in [1,3]. As a sub problem of the "proxy problem", Neuman [2] proposed two schemes for delegating signature rights: "bearer proxy" and "delegated proxy".

Mambo, et al. [3] gave a systematic discussion of proxy signatures. They mentioned three levels of delegation:

Full delegation: The original signer gives its private key to the proxy signer.

Partial delegation: The original signer generates a proxy signature key from its private key and gives it to the proxy signer. The proxy uses the proxy key to sign. The verification equation for proxy signature is modified, so that the proxy signature is distinguishable from the signature created by the original signer.

Delegation by warrant: Warrant is a certificate composed of a message part and a public signature key. The proxy signer obtains the warrant from the original signer and uses the corresponding private key to sign. The resulting signature consists of the created signature and the warrant

One of the ways to delegate was as follows [3]: The original signer sent a certificate containing a key to the proxy signer. The proxy signer used this key to proxy-sign. The proxy signer attached the certificate in every signature to authenticate itself. The above was an example of *consecutive execution*, which combines common cryptographic primitives in modular fashion to achieve the objectives. Ways to achieve the same objectives by directly modifying the signature equations were also presented in [3], an approach that was called *direct form*. Better performances than those schemes in [2] were achieved.

The proxy signature of Kim, et al. [4] included a warrant in the proxy signature. The original signer gained the ability to restrict the message types that are delegated. The warrant included the proxy's identity which prevented the transfer of proxy power to another party.

The proxy signature scheme of Lee, et al. [5] did not explicitly include the identity of the proxy signer in the warrant. In particular, the proxy signer could independently generate proxy key pairs valid for message types in conformance with the warrant. Schemes in [4] and [5] expose the identity of the proxy signer in the signature.

The schemes in [3,4,5] were DL-based. There were also proxy signature schemes based on RSA equations [6,7,9]. Sander, et al. [7] suggested the use of encrypted functions to achieve undetachable signatures. Kotzanikolaous, et al. [9] realized that suggestion. Lee, et al. [6] further extended it to support strong non-repudiation by including the proxy signer's public key in the verification equations.

Our Contribution: The signature schemes in Lee, et al. [5] achieved the first five of the following seven properties. The main contribution of this paper is to present an extension which achieves all seven properties except Property 5.

1. **Verifiability**: The original signer's delegation on the signed message is verifiable using publicly available parameters.
2. **Strong unforgeability**: It is difficult to forge a specific proxy's signature, even by the original signer.
3. **Strong non-repudiation**: It is difficult for a proxy signer to repudiate its signatures against any verifier.
4. **Non-designated**: The warrant issued by the original signer is transferable among proxy signers.
5. **Strong identifiability**: A proxy signer's identity can be determined from a proxy signature it performs.
6. **Proxy privacy**: The proxy signer's identity cannot be revealed from its signatures alone.

Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02)
1080-1383/02 $17.00 © 2002 **IEEE**

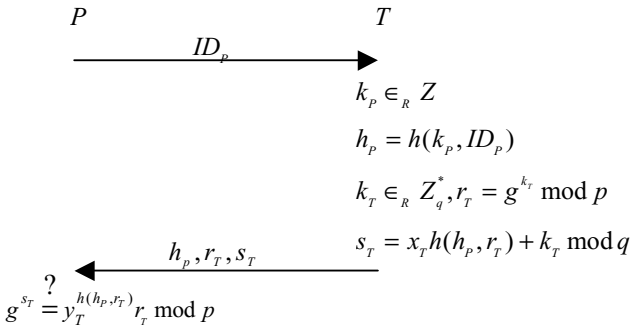
7. **Privacy revocation**: If needed, a proper authority can determine the identity of the proxy signer of a document from the signature.

II. Our Scheme

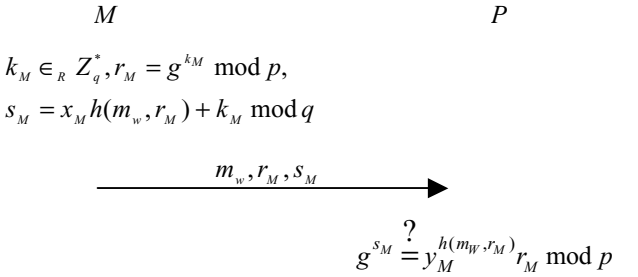
Our proxy signature scheme protects the privacy of proxy signers by certified aliases. We have a trusted Alias Issuing Authority *T*, the original signer *M*, the proxy signer *P,* and the signature verifier *V*.

Discrete Logarithm (DL) parameters: Let p, q be prime numbers with $q \mid (p-1)$, g be an element of order q in the multiplicative group Z_p^*, $h(\bullet)$ be a secure hash function. Let σ=sign(*m,s*) be a DL-based signature algorithm and $verify(m, \sigma, v)$ be the corresponding verification algorithm, for message *m*, private key *s*, and public key *v*. The key pairs of *T* and *M* are $(x_T, y_T = g^{x_T})$ and $(x_M, y_M = g^{x_M})$, respectively. The public keys y_T and y_M are known to all.

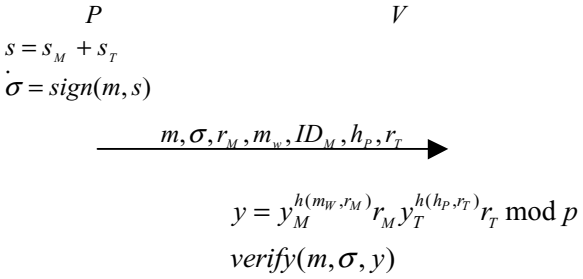
Issuing Alias: *T* issues an alias h_P to *P*, along with parameters r_T, s_T for *P* to verify the validity of the alias. *T* records all triple (h_P, k_P, ID_P) for later privacy revocation needs.



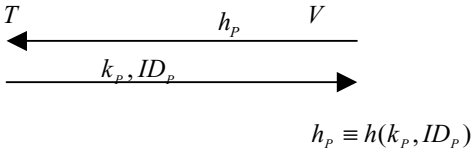
Delegating: *M* generates a proxy key pair (s_M, g^{s_M}), sends it to *P* along with validity proof m_W, r_M.



Sign and verify: *P* signs by combining its two secrets s_M and s_T. *V* verifies by using public keys of *T* and *M*.



Revoking privacy: When needed, *T* revokes *P*'s privacy.



In conclusion, certified alias can be used to protect the privacy of the proxy signer. Both anonymity and identifibility are achieved. Due to space limitations, security analyses are left to [10].

References

[1] V. Varadharajan, P. Allen, and S. Black, "An analysis of the proxy problem in distributed systems." *Proc. IEEE Computer Society Symp. on Research in Security and Privacy*(1991) 255-275.

[2] B. C. Neuman, "Proxy-based authorization and accounting for distributed systems." *Proc 13th International Conference on Distributed Computing Systems* (1993) 283-291.

[3] M. Mambo, K. Usuda, and E.Okamoto, "Proxy Signature: Delegation of the Power to Sign Messages." *IEICE Trans. Fundamentals*, **E79-A**:9 (1996) 1338-1353.

[4] S. Kim , S. Park, and D. Won, "Proxy Signature, revisited." *Proc of ICICS' 97 , International Conference on Information and Communication Security* (1997) 223-232.

[5] B. Lee, H. Kim, and K. Kim, "Strong Proxy Signature and its Applications." *Proc of SCIS 2001* (2001) 603-608.

[6] B. Lee, H. Kim, and K. Kim, "Secure Mobile Agent using Strong Non-designated Proxy Signature." *Proc. ACISP* (2001) 474-486.

[7] T. Sander and C. Tschudin, "Towards Mobile Cryptography." *Tech. Rep. 97-409, Int'l Computer Science Inst., Berkeley* (1997).

[8] D. Chaum and E. van Heijst, "Group signatures*.", Advances in Cryptology - Eurocrypt '91* (1991) 257-265.

[9] P. Kotzanikolaous, M. Burmester, and V. Chrisskopoulos, "Secure Transactions with Mobile Agents in Hostile Environments", *Proc. ACISP 2000, LNCS 1841* (2000) 289-297.

[10] K. Shum, *A Strong Proxy Signature Scheme with Proxy Signer Privacy Protection.* MPhil Thesis, Dep. of Information Engineering, Chinese University of Hong Kong (2002).