Fei LI, Wei GAO, Gui-lin WANG, Ke-fei CHEN, Chun-ming TANG, 2019. Double-authentication-preventing signatures revisited: new definition and construction from chameleon hash. *Frontiers of Information Technology & Electronic Engineering*, 20(2):176-186. https://doi.org/10.1631/FITEE.1700005

Double-authentication-preventing signatures revisited: new definition and construction from chameleon hash

Key words: Double-authentication-preventing signatures; Chameleon hash function; Digital signature; Provable security; Authority trust level

Corresponding author: Fei LI
E-mail: miss_lifei@163.com

ORCID: Fei LI, https://orcid.org/0000-0002-8916-8330

Motivation

The research on DAPS has just begun. In the pioneering work, some basic problems on DAPS are left in theory and in practice. There is only one generic DAPS construction from the so-called extractable 2:1 trapdoor functions with only one instantiation scheme based on the integer factorization assumption. This concrete DAPS signature scheme has much larger signature size and longer running time for signing operation. This study is motivated to focus on some fundamental issues on DAPS in both theory and practice, including, but not limited to, the above problems.

Main idea

1. For DAPS, we propose a new definition for double-signature forgeability. It is slightly weaker than the previous one, but still reasonable since it remains strong enough to ensure the DAP property.

2. For chameleon hash functions, we propose a new notion of the invertible chameleon hash function with key exposure.

3. We propose a provably secure generic framework to construct the DAPS scheme from any invertible chameleon hash function with key exposure, which is much more generic than the previous one.

Construction results comparison

Table 1 Comparison of different double-authentication-preventing signature schemes

Item	PS-DAPS (Poettering and Stebila, 2014)	IF-DAPS (Section 6.1)	RSA-DAPS (Section 6.2)	CDH-DAPS (Section 6.3)
Secret key	p, q	p, q	$d : 1 < d < \phi(n)$	$x : 1 < x < \lvert\langle\mathbb{G}\rangle\rvert$
Public key	$(n, t) : t \in \mathbb{Z}_n^*$	n	$(n, e, y) : y \in \mathbb{Z}_n^*, e > 2^l$	$(g, y, \bar{y}) : g, y, \bar{y} \in \mathbb{G}$
Signature	$(s, a_1, a_2 \ldots, a_l)$: $s, a_i \in \mathbb{Z}_n$	$(r, s) : r \in \mathbb{Z}_n$, $s \in \{0,1\}^l$	$(r, s) : r \in \mathbb{Z}_n$, $s \in \{0,1\}^l$	$(r_1, r_2, s) : r_i \in \mathbb{G}$, $s \in \{0,1\}^l$
Signing	$(l+1)$(Jac + Sqrt)	$(l+1)$(Jac + Sqrt)	2Exp	3Exp′
Verifying	$(l+1)$(Jac + Sqr)	$(l+1)$(Jac + Sqr)	2Exp	1Exp′ + 1DDH
Setup model	Trusted	Trusted	Untrusted	Untrusted
DAP (Section 2)	Extract	Extract	SForge	SForge

Jac: computation of Jacobi symbol modulo n; Sqrt: square root modulo n; Sqr: squaring modulo n; Exp: exponentiation modulo n; Exp′: exponentiation in group $\mathbb{G}$; DDH: verifying the decisional Diffie-Hellman tuple

Conclusions

1. We have proposed a new formalization of the double-signature forgeability which captures the DAP property with looser conditions. The property of invertibility was explicitly proposed for the chameleon hash function with key exposure.

2. We succeeded in constructing the new generic DAPS scheme based on an invertible chameleon hash function with key exposure. Three DAPS schemes based on the common assumptions of IF, RSA, and CDH respectively were instantiated.

3. Due to the rich cryptographic and algebraic properties of the new cryptographic primitive of the invertible chameleon hash function, we expect to discover more applications for other relative cryptographic schemes.