Parametrização de desempenho do esquema de assinatura digital Winternitz e suas variantes

Novembro de 2017

1 Introdução

A utilização de protocolos criptográficos entre dispositivos e entidades é amplamente disseminada e considerada um fator crítico no contexto da validação de quaisquer atos de comunicação realizados por estes indivíduos, em virtude da possível criticalidade e sensibilidade atribuídas aos dados transmitidos. Esquemas de assinatura digital são comumente utilizados para assegurar esta validação de maneira formal [Gol04], através da autenticidade e não-repúdio do remetente e certeza da integridade dos dados em um contexto, a fim de traduzir o resguardo provido por uma assinatura de próprio punho no mundo real.

Na prática, a maior parte destes esquemas utilizam criptossistemas de chave pública baseados em problemas de teoria dos números, como a fatoração de inteiros ou resolução do logaritmo discreto para números grandes. Este fato provê a segurança necessária para os esquemas em computadores clássicos (eletrônicos), em virtude da não-existência de algoritmos de tempo polinomial para a resolução destes problemas. Entretanto, em computadores quânticos, algoritmos dessa forma já existem — em especial, o algoritmo de Shor [Sho97] — efetivamente tornando estes esquemas clássicos inseguros.

Para combater esta situação, a criptografia pós-quântica encarrega-se de buscar algoritmos criptográficos cuja segurança é considerada razoável, mesmo utilizando-se de um computador quântico e ataques especializados, como o algoritmo de Grover [Gro96]. Uma definição viável de esquema de assinatura digital resistente a este tipo de computador pode ser dada apenas com funções de resumo criptográfico, construídas a partir de funções de mão única [KK05]. De fato, estas funções, desde que apresentem requisitos de segurança como resistência à segunda pré-imagem e à colisões, são necessárias e suficientes para a construção de esquemas bem comportados e seguros [Rom90].

Esquemas de assinatura digital baseados em funções de resumo criptográfico consistem da combinação de um esquema de assinatura digital única, onde apenas uma mensagem pode ser assinada de modo seguro, e uma estrutura chamada de árvore de Merkle [Mer89], que abriga diversos pares de chave do esquema supracitado como suas folhas, e reduz a verificação destes para uma única chave, codificada em sua raiz. Esta árvore é construída com a concatenação de resumos criptográficos do conteúdo dos nós, habilitando assim a assinatura de diversas mensagens. Como uma função específica não é necessária, é possível obter uma grande variedade de esquemas, garantindo a versatilidade desta abordagem.

Embora os esquemas iniciais tenham sido construídos sem atenção particular à eficiência de modo geral (e.g. o esquema de assinatura única de Lamport-Diffie [Lam79] assina apenas um *bit* de informação em sua forma mais simples), muitos resultados práticos demonstram a redução contínua do tempo de verificação da assinatura, tamanho e tempo para geração do par de chaves e assinatura, bem como avanços teóricos possibilitam a utilização de funções com requisitos de segurança mínimos, garantem o conceito de sigilo encaminhado [BDH11] (i.e. comprometimento de uma chave não implica na segurança de mensagens que utilizaram esta chave anteriormente) e da ausência de estado [BHH+15] (i.e. esquema não necessita registrar quais chaves de assinatura única já foram utilizadas).

2 Motivação

O esquema de assinatura digital única Winternitz é proposto como uma generalização de [Lam79], permitindo a assinatura de múltiplos *bits* simultaneamente. Tal comportamento é configurado por um parâmetro w, que implica imediatamente no tamanho do par de chaves e na velocidade que a assinatura é criada e/ou verificada. Com um parâmetro w bem escolhido, o esquema torna-se relativamente eficiente, e a valer, este e sua variante WOTS+ [Hül17], cujos requisitos de segurança são diminuídos, têm sido utilizados amplamente como parte de diversos esquemas baseados em funções de resumo criptográfico, como SPHINCS [BHH+15], MSS [Mer89], CMSS [BCGD+06], GMSS [BDK+07] e XMSS [BDH11].

Como descrito em [BBD08], o algoritmo consiste na aplicação da função de resumo criptográfico escolhida repetidamente sobre blocos da chave privada, i.e. um encadeamento da função. O número de blocos é decidido pelo parâmetro w e representará quantos bits serão assinados simultaneamente, bem como o tamanho máximo da cadeia de resumos para um bloco $(2^w - 1)$. Para realizar a assinatura de cada bloco, é preciso determinar a quantidade de vezes que o encadeamento será repetido. Isto pode ser feito obtendo uma fração de w *bits* do resumo criptográfico da mensagem que deseja-se assinar. Uma assinatura, portanto, é um conjunto de cadeias de resumos criptográficos da chave privada.

Winternitz figura como o esquema escolhido para assinar as folhas das árvores de grande parte da literatura prática em cima de esquemas baseados nesta estrutura de dados. Por exemplo, no caso do SPHINCS, construído em cima do conceito de camadas de árvores de Merkle (a fim de descartar a necessidade de manter o estado do esquema de assinatura digital), WOTS+ é utilizado para a autenticação entre estas. Afirma-se, então, que é um dos esquemas de assinatura única mais populares, tanto em resultados práticos como teóricos – denotando um interesse da comunidade acadêmica por resultados que impliquem em melhorias no algoritmo.

3 Contribuições propostas

Devido à construção do algoritmo, e como os processos de geração de chaves, assinatura e verificação são realizados, demasiadas aplicações da função de resumo criptográfico escolhida são realizadas na vida útil de uma assinatura digital. Assim, uma possível fronte

de pesquisa consiste na utilização ótima de recursos computacionais na computação de resumos criptográficos para que o desempenho de Winternitz, e consequentemente de outros esquemas baseados em funções de resumo criptográfico, seja melhorado.

Ademais, como a saída de uma função de resumo criptográfico deve conter, em média, o mesmo número de 0s e 1s, é possível concluir que metade do processo de encadeamento estará localizado na geração da assinatura, e a outra metade na verificação. Entretanto, em situações onde assinaturas são raramente produzidas mas frequentemente verificadas, e vice-versa, esta distribuição de cômputos torna o processo não otimizado, de modo a sugerir uma possível alteração no comportamento do algoritmo a fim de considerar estes diversos casos de uso.

Isto implica na introdução de técnicas determinísticas a fim de modificar o processo de encadeamento de resumos. O trabalho de [SV08] propõe um esquema de assinatura digital baseado em Winternitz utilizando compressão de cadeias repetidas (*run-length encoding*) que resulta na diminuição em 33% do tempo de verificação para uma assinatura, com $w < 4$; diferentemente deste esquema, propõe-se a criação de passos adicionais ao Winternitz convencional, na etapa de geração da assinatura, a fim de customizar o tamanho da cadeia de resumos e obter um resultado paramétrico à situação desejada. Implementações iniciais demonstram o mesmo ganho relativo, mas para valores de w maiores, implicando em ganhos absolutos mais significativos, visto que o número de resumos criptográficos cresce exponencialmente em função deste parâmetro.

4 Possíveis orientadores

1. Ricardo Felipe Custódio
   Linha de pesquisa — Segurança em Sistemas Computacionais;
2. Jean Everson Martina
   Linha de pesquisa — Segurança em Sistemas Computacionais.

Referências

[BBD08] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen. *Post Quantum Cryptography*. Springer Publishing Company, Incorporated, 1st edition, 2008.

[BCGD+06] Johannes Buchmann, Luis Carlos Coronado García, Erik Dahmen, Martin Döring, and Elena Klintsevich. CMSS – An Improved Merkle Signature Scheme. In Rana Barua and Tanja Lange, editors, *Progress in Cryptology - INDOCRYPT 2006*, pages 349–363, Kolkata, India, 2006. Springer-Verlag Berlin Heidelberg.

[BDH11] Johannes Buchmann, Erik Dahmen, and Andreas Hülsing. XMSS - a Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. In *Proceedings of the 4th International Conference on Post-Quantum Cryptography*, PQCrypto'11, pages 117–129, Berlin, Heidelberg, 2011. Springer-Verlag.

[BDK+07] Johannes Buchmann, Erik Dahmen, Elena Klintsevich, Katsuyuki Okeya, and Camille Vuillaume. Merkle Signatures with Virtually Unlimited Signature Capacity. *Lecture Notes in Computer Science*, 4521:31–45, 2007.

[BHH+15] Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O'Hearn. SPHINCS: Practical Stateless Hash-Based Signatures. In *Advances in Cryptology – EUROCRYPT 2015*, pages 368–397. Springer-Verlag Berlin Heidelberg, 2015.

[Gol04] Oded Goldreich. *Foundations of Cryptography: Volume 2, Basic Applications*. Cambridge University Press, New York, NY, USA, 2004.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 212–219, New York, NY, USA, 1996. ACM.

[Hül17] Andreas Hülsing. WOTS+ – Shorter Signatures for Hash-Based Signature Schemes. Cryptology ePrint Archive, Report 2017/965, 2017. http://eprint.iacr.org/2017/965.

[KK05] Jonathan Katz and Chiu-Yuen Koo. On Constructing Universal One-Way Hash Functions from Arbitrary One-Way Functions. Cryptology ePrint Archive, Report 2005/328, 2005. http://eprint.iacr.org/2005/328.

[Lam79] Leslie Lamport. Constructing Digital Signatures from a One Way Function. *SRI International*, 1979.

[Mer89] Ralph C. Merkle. A Certified Digital Signature. In *Proceedings on Advances in Cryptology*, CRYPTO '89, pages 218–238, New York, NY, USA, 1989. Springer-Verlag New York, Inc.

[Rom90] J. Rompel. One-way Functions Are Necessary and Sufficient for Secure Signatures. In *Proceedings of the Twenty-second Annual ACM Symposium on Theory of Computing*, STOC '90, pages 387–394, New York, NY, USA, 1990. ACM.

[Sho97] Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.*, 26(5):1484–1509, October 1997.

[SV08] Rainer Steinwandt and Viktória I. Villányi. A One-time Signature Using Run-length Encoding. *Inf. Process. Lett.*, 108(4):179–185, October 2008.