# Ring Signatures for Deniable AKEM: Gandalf's Fellowship

Phillip Gajland[1,2], Jonas Janneck[2], Eike Kiltz[2]

[1]Max Planck Institute for Security and Privacy
[2]Ruhr University Bochum

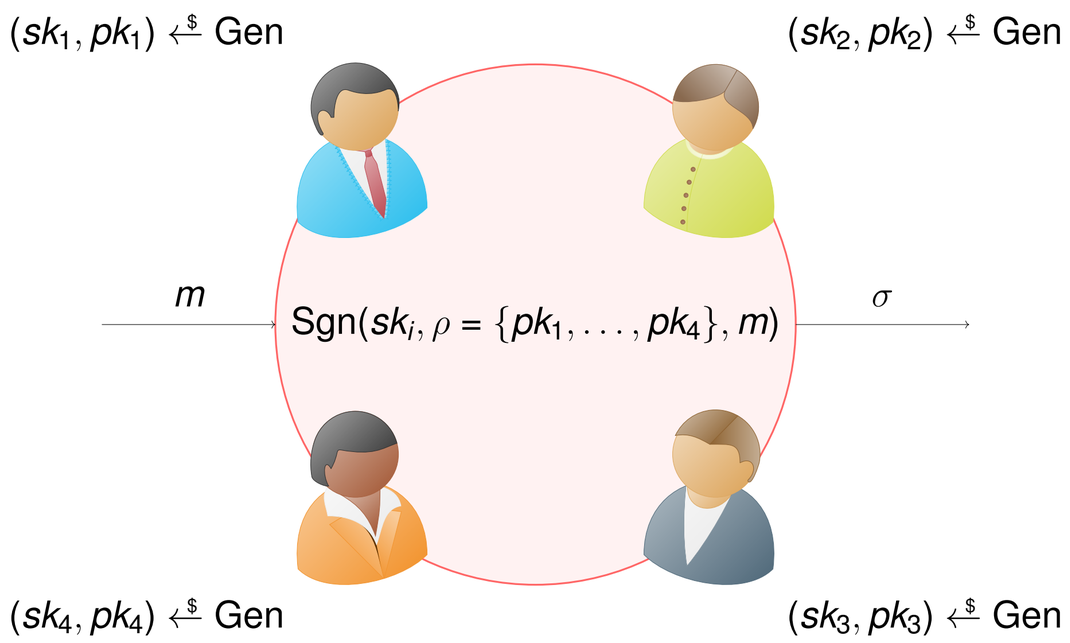
https://ia.cr/2024/890

Accepted at *CRYPTO '24*.

MAX PLANCK INSTITUTE FOR SECURITY AND PRIVACY

## Ring Signature Scheme [RST01]

RSig = (Gen, Sgn, Ver)

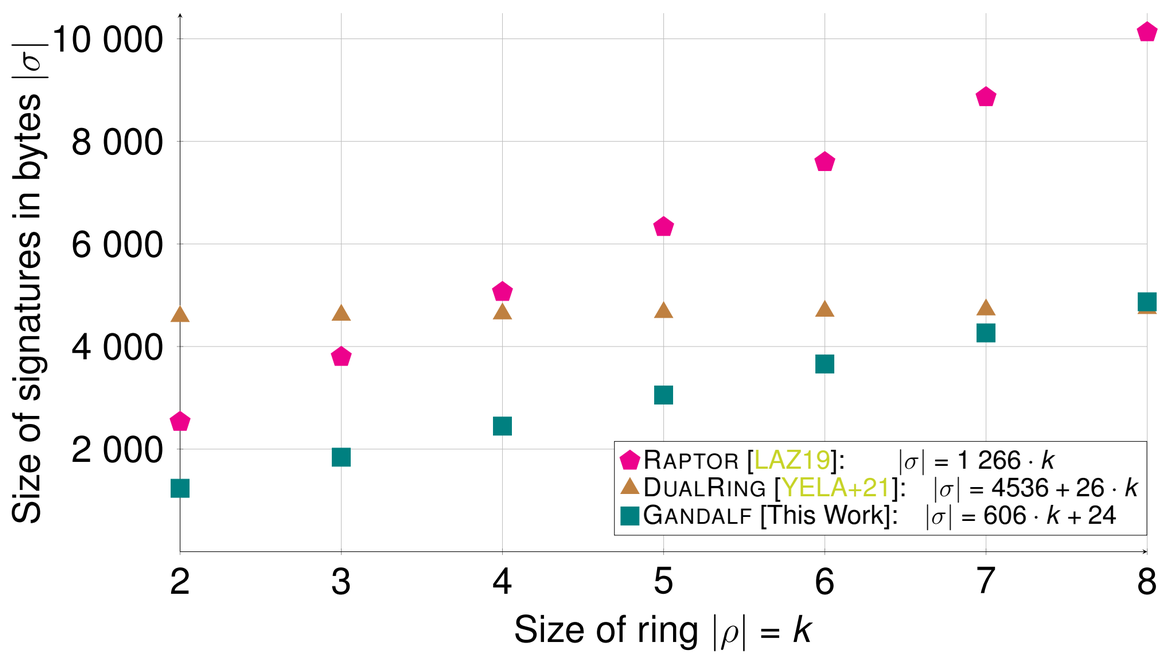



- Ring signatures [RST01] allow users to sign messages on behalf of dynamically formed user groups, and are publicly verifiable while preserving the signer's anonymity within the group (signing ring $\rho$).
- Ring signatures are widely adopted in blockchains and voting systems.
- Recent works achieve asymptotic signature size $\mathcal{O}(\log(|\rho|))$ using proof systems. However, for applications involving small rings, linear schemes are preferable.
- We construct a ring signature scheme, GANDALF, specifically for small rings, providing 50% reduction in signature sizes over the state of the art.

- GANDALF, is based on the NTRU pre-image sampleable trapdoor function $f_h$ [GPV08] over the NTRU ring.
- Concretely, $f_h$ inputs two ring elements of small norm and is defined as $f_h(u, v) = h * u + v$. A valid ring signature on message $m$ for the ring $\rho = \{h_1, \ldots, h_k\}$ consists of a vector $(u_1, \ldots, u_k) \in \mathcal{R}^k$ such that

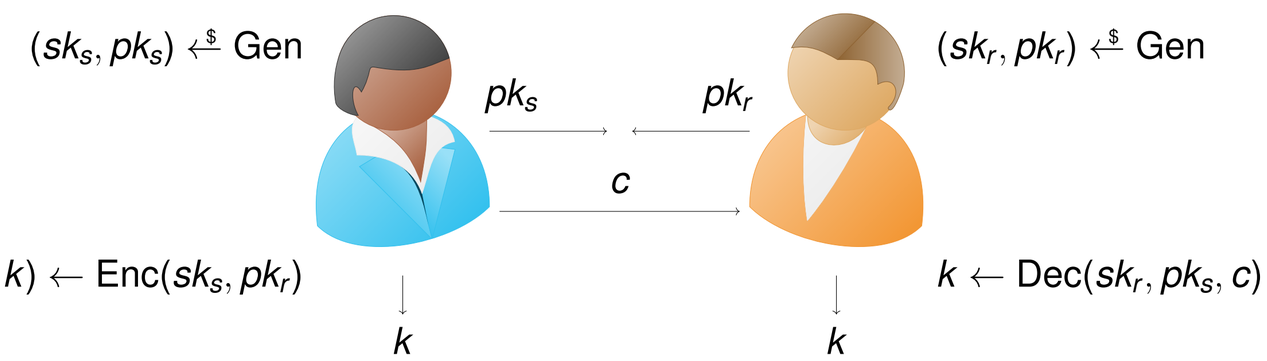
$$\left\| \left( u_1, \ldots, u_k, v = \mathsf{H}(m, \rho) - \sum_{i=1}^{k} h_i * u_i \right) \right\|_2 \leq \beta.$$

- The ring signature essentially consists of $k$ "unseeded FALCON signatures" [PFHK+22] and ring element $v$ is implicitly reconstructed in the verification equation.




## Deniable Authenticated Key Exchange Mechanisms (AKEM) [ABHK+21]

AKEM = (Gen, Enc, Dec)




- An AKEM can be thought of the KEM analogue of signcryption and was first formalised in [ABHK+21]. It is the primitive behind the recent HPKE [BBLW22] standard used in MLS and TLS.
- Our work introduces and formalises deniability for the AKEM primitive.
- Furthermore, we show a black box construction of a deniable AKEM using our ring signature scheme.

| | | Honest Receiver | | Dishonest Receiver | |
|---|---|---|---|---|---|
| | | $sk_r$ does not leak | $sk_r$ leaks | $sk_r$ does not leak | $sk_r$ leaks |
| Honest Sender | $sk_s$ does not leak | $\mathrm{Sim}(\emptyset), \mathcal{A}(\emptyset)$ | $\mathrm{Sim}(\emptyset), \mathcal{A}(sk_r)$ | $\mathrm{Sim}(sk_r), \mathcal{A}(\emptyset)$ | $\mathrm{Sim}(sk_r), \mathcal{A}(sk_r)$ |
| | $sk_s$ leaks | $\mathrm{Sim}(\emptyset), \mathcal{A}(sk_s)$ | $\mathrm{Sim}(\emptyset), \mathcal{A}(sk_s, sk_r)$ | $\mathrm{Sim}(sk_r), \mathcal{A}(sk_s)$ | $\mathrm{Sim}(sk_r), \mathcal{A}(sk_s, sk_r)$ |

| Primitive | Scheme (variant) | Security | Model | Size (in bytes) | | |
|---|---|---|---|---|---|---|
| | | | | $\sigma$ | $c$ | $pk$ |
| RSig | GANDALF [this work] | **UF**, **Ano** | ROM | 1 244 | — | 896 |
| KEM | NTRU-A [DHKL+23] | **IND-CCA** | QROM | — | 768 | 768 |
| AKEM | AKEM [this work] | **Ins-Aut**, **Ins-CCA** **HR-Den**, **DR-Den** | Standard | — | 2 012 | 1 664 |

[DHKL+23] Julien Duman, Kathrin Hövelmanns, Eike Kiltz, Vadim Lyubashevsky, Gregor Seiler and Dominique Unruh. "A Thorough Treatment of Highly-Efficient NTRU Instantiations". In: *Public-Key Cryptography – PKC 2023*. 2023.

[BBLW22] Richard Barnes, Karthikeyan Bhargavan, Benjamin Lipp and Christopher A. Wood. *Hybrid Public Key Encryption*. RFC 9180. 2022.

[PFHK+22] Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte and Zhenfei Zhang. *FALCON*. Tech. rep. available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022. National Institute of Standards and Technology, 2022.

[ABHK+21] Joël Alwen, Bruno Blanchet, Eduard Hauck, Eike Kiltz, Benjamin Lipp and Doreen Riepel. "Analysing the HPKE Standard". In: *Advances in Cryptology – EUROCRYPT 2021*. 2021.

[YELA+21] Tsz Hon Yuen, Muhammed F. Esgin, Joseph K. Liu, Man Ho Au and Zhimin Ding. "DualRing: Generic Construction of Ring Signatures with Efficient Instantiations". In: *Advances in Cryptology – CRYPTO 2021*. 2021.

[LAZ19] Xingye Lu, Man Ho Au and Zhenfei Zhang. "Raptor: A Practical Lattice-Based (Linkable) Ring Signature". In: *Applied Cryptography and Network Security*. 2019.

[GPV08] Craig Gentry, Chris Peikert and Vinod Vaikuntanathan. "Trapdoors for hard lattices and new cryptographic constructions". In: *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*. 2008.

[RST01] Ronald L. Rivest, Adi Shamir and Yael Tauman. "How to Leak a Secret". In: *Advances in Cryptology — ASIACRYPT 2001*. 2001.