From: Apon, Daniel C. (Fed)
To: Robinson, Angela Y. (Fed)
Subject: Re: a buffet of abstracts to choose from!
Date: Monday, September 27, 2021 12:40:32 PM

(or it could be that it is just a longer paper or something -- who knows)

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Monday, September 27, 2021 12:38 PM
To: Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>
Subject: Re: a buffet of abstracts to choose from!

likely, there's some kind of conflict of interest or other social scenario going on even before the paper is reviewed

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Monday, September 27, 2021 12:37 PM
To: Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>
Subject: Re: a buffet of abstracts to choose from!

fyi-- for no apparent reason that i can see, #33 is one of 2 papers I was assigned that has 5 reviewers assigned instead of the usual 3 (whatever that means)

From: Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>
Sent: Monday, September 27, 2021 12:18 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Subject: RE: a buffet of abstracts to choose from!

I'll take #33 please!

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Monday, September 27, 2021 12:16 PM
To: Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>
Subject: a buffet of abstracts to choose from!

Pick your poison.. =)

(I've been handing out 1 per person so far, but if you find more than 1 interesting, you can have 2.. -- as a PC member, I feel obligated to review a large chunk of my assignments myself)

#27 Lattice-based Signatures with Tight Adaptive Corruptions and More

Abstract:

We construct the first tightly secure signature schemes in the multi-user setting with adaptive corruptions from lattices. In stark contrast to the previous tight constructions whose security is solely based on number-theoretic assumptions, our schemes are based on the Learning with Errors (LWE) assumption which is supposed to be post-quantum secure. The security of our scheme is independent of the numbers of users and signing queries, and it is in the non-programmable random oracle model. Our LWE-based scheme is compact, namely, its signatures contain only a constant number of lattice vectors.
At the core of our construction are a new abstraction of the existing lossy identification (ID) schemes using dual-mode commitment schemes and a refinement of the framework by Diemert et al. (PKC 2021) which transforms a lossy ID scheme to a signature using sequential OR proofs. In combination, we obtain a tight generic construction of signatures from dual-mode commitments in the multi-user setting. Improving the work of Diemert et al., our new approach can be instantiated using not only the LWE assumption, but also an isogeny-based assumption. We stress that our LWE-based lossy ID scheme in the intermediate step uses a conceptually different idea than the previous lattice-based ones.
Of independent interest, we formally rule out the possibility that the aforementioned ``ID-to-Signature'' methodology can work tightly using parallel OR proofs. In addition to the results of Fischlin et al. (EUROCRYPT 2020), our impossibility result shows a qualitative difference between both forms of OR proofs in terms of tightness.

#33 On the Efficiency and Flexibility of Signature Verification

Abstract:

Digital signatures are a well-established means to securely certify data integrity and authenticate sources. One core component of digital signature schemes is signature verification. Traditionally, verification is monolithic and returns a decision (accept/reject) only at the very end of the process. In this work, we pose two questions that dismantle this monolithic view on signature verification: (1) is it possible to extract meaningful information from a partial verification? (flexibility); and (2) is it possible to split the verification process into a computational heavy, one-time set-up, and a lightweight, reusable part, without undermining unforgeability? (effciency). We answer both questions in a positive way for specific classes of schemes that include post-quantum secure signatures from lattices and from multivariate polynomials. We develop formal frameworks for signatures with effcient verification, flexible verification, and combinations of the two. Crucially, we regard these as features that may enhance existing constructions, rather than requiring a re-design. For each framework, we exhibit generic transformations to realize effcient (and/or) flexible verification for signature schemes that involve a matrix-vector multiplication among the checks. Our transformations apply to the NIST finalist Rainbow; MP12 (EUROCRYPT); GVW15 (STOC); and Lyub12 (EUROCRYPT) when implemented with non-cryptographic hash functions as suggested by Chen et al. (CRYPTO21), among other schemes.

#38 Light the Signal: Bounds and Optimization of Signal Leakage Attacks against LWE-Based Key Exchange

Abstract:

Signal leakage attacks against LWE-based key exchange have drawn a lot of attention. Recently, Bindel, Stebila, and Veitch proposed a sparse signal collection method to attack some key reuse robustness schemes such as DBS-KE and DBS-AKE, improving the known signal leakage attacks by greatly reducing the number of queries. However, the number of queries in their attacks is still huge. In this paper, we consider the attack with the least number of queries. By converting the problem of launching a signal leakage attack into a coding problem, we first propose lower bounds for the least number of queries in some signal leakage attacks. Inspired by our proposed bounds, we also propose a generic Targeted Signal Extraction method, which significantly reduces the queries needed for the signal leakage attacks on LWE-based key exchange scheme DXL-KE and the key reuse robustness scheme DBS-KE. Further, we propose a complete key recovery attack against the password-based authenticated key exchange scheme LBA-PAKE with only 757 queries. The experiments show that our proposed method is effective and efficient. Our attack demonstrates that it is still a challenging task to design lattice-based authenticated key exchange schemes in the face of key reuse attacks.

#67 Ring Key-Homomorphic Weak PRFs and Applications

Abstract:

A weak pseudorandom function F:K x X -> Y is said to be ring key-homomorphic if, given F(k_1,x) and F(k_2,x), there are efficient algorithms to compute F(k_1 + k_2,x) and F(k_1 * k_2,x) where + and * are the addition and multiplication

operations in the ring K, respectively. In this work, we initiate the study of ring key-homomorphic weak PRFs (RKHwPRFs). In particular, we show that the following primitives can be constructed from any RKHwPRF:
- Multiparty noninteractive key exchange (NIKE) for an arbitrary number of parties.
- Indistinguishability obfuscation for all circuits in NC_1.

Our proofs are in the standard model, and the proof for our iO scheme is program-independent. Our iO scheme can also be bootstrapped to all polynomial-size circuits using standard techniques. We also consider restricted versions of RKHwPRFs that are structurally weaker than a classic RKHwPRF but suffice for all our constructions. We show how to instantiate these restricted RKHwPRFs from various multilinear maps and associated assumptions. Our framework gives several new results, such as:
- The first iO scheme that relies only on SXDH over any asymmetric multilinear map without additional assumptions.
- The first iO scheme that relies only on DLIN (or more generally Matrix-DDH) over any (even symmetric) multilinear map without additional assumptions.
- The first iO scheme that relies on SXDH over the multilinear map presented by Ma and Zhandry (TCC'18) (the authors only presented a NIKE protocol in their paper). To our knowledge, this candidate multilinear map has not been successfully cryptanalyzed, and the SXDH assumption plausibly holds over it.

Our analysis of RKHwPRFs in a sense completes the work initiated by Alamati et al. (EUROCRYPT'19) on building cryptosystems from generic Minicrypt primitives with structure. With our results, almost all of the major known cryptosystems can be built from a weak PRF with either a group or ring homomorphism over either the input space or the key space. Thus, a major contribution of this work is advancing the study of the relationship between structure and cryptography.

#79   Generic, Efficient and Isochronous Gaussian Sampling over the Integers

Abstract:

Gaussian sampling over the integers is one of the fundamental building blocks of lattice-based cryptography. Among the extensively used trapdoor sampling algorithms, it's ineluctable until now. Under the influence of numerous side-channel attacks, it's still challenging to construct a Gaussian sampler that is generic, efficient, and resistant to timing attacks. In this paper, our contribution is three-fold.

First, we propose a secure, efficient exponential Bernoulli sampling algorithm. It can be applied to Gaussian samplers based on rejection samplings. We apply it to FALCON, a candidate of round 3 of the NIST post-quantum cryptography standardization project, and reduce its signature generation time by 13%-14%. Second, we develop an isochronous Gaussian sampler based on rejection sampling. Our Algorithm can securely sample from Gaussian distributions with different standard deviations and arbitrary centers. We apply it to PALISADE (S&P 2018), an open-source lattice cryptography library. During the online phase of trapdoor sampling, the running time of the G-lattice sampling algorithm is reduced by 44.12% while resisting timing attacks.

Third, we improve the efficiency of the COSAC sampler (PQC 2020). The new COSAC sampler is 1.46x-1.63x faster than the original and has the lowest expected number of trials among all Gaussian samplers based on rejection samplings. But it needs a more efficient algorithm sampling from the normal distribution to improve its performance.