QIC 891 Topics in Quantum Safe Cryptography

Module 1: *Post-Quantum Cryptography*

Lecture 3

Lecturer: Fang Song *May 17, 2016*

Review. Signature without trapdoors.
Today. We'll introduce trapdoor functions(TDF) and realizations from post-quantum assumptions. Using TDFs we will see another generic construction for signature schemes. We will then use TDFs to construct public-key encryption schemes.

1 Trapdoor functions

We've played with functions that are assumed to hard to invert. In many cryptographic applications, it will be extremely useful to have some side information, usually kept secret and called a "trapdoor", with which one can invert the function efficiently. We call such functions trapdoor (one-way) functions, denoted $(f,(f^{-1},td))$ where td represents the trapdoor and $f^{-1}(td,\cdot)$ is an efficient inverting algorithm. We often just write f^{-1} and view td as implicit. (Formally speaking, we should define *family* of functions.)

Notice that for the functions induced from the coding problems and MQ problems already possess trapdoors due to the specific way we constructed them. For instance recall the syndrome decoding problem we set $H := H_0P$ where

- $H_0 \in \mathbb{F}_2^{(n-k)\times n}$: a parity check matrix for a linear code with an efficient docoding algorithm D_0. Namely given a syndrome vector $s \in \mathbb{F}_2^{n-k}$, D_0 finds an error vector $e \leftarrow D_0(y)$ with weight $\|e\| = \beta$.
- $P \in_R S_n$: a random permutation matrix.

Let $g_H : x \mapsto Hx$ and $td := (D_0, P)$. Then with td it is easy to invert g_H.

1.1 Lattice trapdoors

Embedding trapdoors in lattice problems needs more work[1]. Roughly speaking there are two types of lattice trapdoors:

I **"Short-basis"** trapdoors: introduced and developed in [GGH97, GPV08, CHKP12]. A very natural & generic technique.

II **"Gadget-matrix"** trapdoors: introduced by [MP12]. They are specific to SIS/LWE (& their Ring-analogues) but usually lead to more efficient computations than type-I.

We'll introduce the type-I trapdoor here in an algebraic way. A more intuitive (geometric) interpretation, which explains the name "short-basis", will be discussed next time.

Basically the trapdoor is a set of independent solutions $\{s_i \in \mathbb{Z}_q^m\}$ for the (homogeneous)SIS problem: $Ax = 0 \pmod q$.

[1] This extra complication should not be viewed as a drawback of lattice-based cryptography. Instead of starting from an easy instance and applying some "ad-hoc" randomization procedure trying to "obfuscate" the easy instance (though some early work did so e.g., [GGH97]), (modern) functions based on lattices (e.g. SIS & LWE) are generated according to cerntain distributions so that inverting these functions can be shown to be as hard as solving some lattice problems in the *worst-case*.

Definition 1 (Type-I lattice trapdoor)**.** *For a matrix $A \in \mathbb{Z}_q^{n\times m}$, $S \in \mathbb{Z}_q^{m\times m}$ is a trapdoor for A if*

1. $AS = 0 \pmod q$
2. *S is full rank over $\mathbb{Z}$.*
3. *$\|S\|$ small, i.e., each collumn $s_i \in \mathbb{Z}_q^m$ is "short".*

Observe that with S, one can solve (in addition to solve homogeneous SIS trivially):

- (inhomogeous) SIS: Given $f_A(x) = Ax \pmod q = y$, there are efficient procedures to find a x' with small norm $\|x'\| \le \beta$ such that $f_A(x') = y \pmod q$ (essentially a *Bounded Distance Decoding* problem as we will see next time). Actually Gentry et al. [GPV08] showed a way to sample a solution according to some canonical distribution, which give what they termed *preimage-samplable functions*. This will be very useful to construct signature schemes (Sect. 2.2).
- LWE: Given $g_{A^T}(s,e) = A^T s + e \pmod q = b$, we have $z := S^T b \pmod q = (AS)^T \cdot s + S^T e = S^T e \pmod q$. However since $\|S\|$ and $\|e\|$ are both small, $z = S^T e$ holds over the integers. Hence we can compute $e = (S^T)^{-1} z$ over $\mathbb{Z}$ and recover s afterwards. This is essentially the injective trapdoor function in [GPV08], which uses LWE to instantiate an early idea in [GGH97].

But how do we generate a trapdoor S? Note that it is not feasible if we sample A uniformly at random and they try to find S. [Why?] Instead, we would generate A and S at the same time, and make sure that A is statistically close to uniform.

Theorem 1 (Generating lattice problems with trapdoor [Ajt99, AP11, MP12])**.** *There is an efficient randomized algorithm that, given positive integers $n, q, m \ge cn\log q$, generates an (almost) uniformly random $A \in \mathbb{Z}_q^{n\times m}$ and a full-rank $S \in \mathbb{Z}_q^{m\times m}$ with $AS = 0 \mod q$ & $\|S\| = O(\text{poly}(n, \log q))$.*

2 Signing with trapdoors

Now that we have trapdoor (one-way) functions available, a natural idea to construct a signature scheme is to use the trapdoor as a secret key so we can sign and verify as:

$$\sigma = S(sk, m) = f^{-1}(td, m); \quad V(m, \sigma) : f(m) \stackrel{?}{=} \sigma .$$

In some textbook, this idea is implemented by the RSA function $f(x) := x^e \pmod N$, $f^{-1}(y) := y^d \pmod N$ where d is the trapdoor. But unfortunately this is not a wise way. Some early lattice based signatures essentially followed this approach [GGH97, HPS01, HHGP+03], which were later broken [GS02, NR09, DN12]. Many code-based and MQ-based schemes also fall into this category.

2.1 Full-Domain Hash

A nuatural idea (which is also a common practice) is to hash a message before signing (e.g., using the "text-book" RSA approach). This indeed gives a secure scheme in the *random-oracle* (RO) model using a trapdoor (one-way) *permuation*. This is formalized as *Full-Domain Hash* [BR93, BR96].
Note on Random-Oracle model. Recall that the RO model assumes a hash function $\mathcal{O}$ that is

1. **Publicly available as a black-box**: anyone, including an adversary, can only evaluate $\mathcal{O}(\cdot)$ by querying.

2. **Behaving completely random**: $\mathcal{O} \in_R \mathcal{F}$ is drawn uniformly from all possible functions from the domain to range.

In addtition to these conditions, proving security in the random oracle model actually employs other tricks. In practice when we implement $\mathcal{O}$ with a concrete hash function (e.g., SHA), the security of the scheme may beomce unjustified. Indeed, there is theoretical result showing that there exists some (contrived) scheme that is secure in RO but is insecure no matter what concret hash function we use to instantiate the RO [CGH04]. However, for natural schemes the RO heuristic is still widely used and has not witnessed any weakness (so far).

Full-doman Hash construction. Given (f, f^{-1}) as a trapdoor (one-way) *permutation*, a hash function $\mathcal{O}$ modeled as an RO whose outputs fall into the codomain of f. We construct a signature scheme $\Sigma = (G, S, V)$ as follows

Full Domain Hash

KeyGen $G(1^\lambda)$:	**Sign** $S(m, sk)$:	**Vrfy** $V(m, \sigma)$:
$pk := f, sk := f^{-1}$.	• Query $\mathcal{O}$ on m and get $y := \mathcal{O}(m)$, • Compute $\sigma := f^{-1}(y)$. Output σ.	• Query and obtain $y = \mathcal{O}(m)$. • Accept iff. $f(\sigma) = y$.

Intuitively, a signature on m is just a random domain element of f which leaks no information about the secret key (trapdoor). To forge a signature (without knowning f^{-1}), an adversary would need to invert a random output y of f, which is assumed to be hard. A crucial point in the formal proof relies on a simple property enabled by the fact that f (and hence f^{-1} too) is a *permutation*. Namely the following two procedures are indistinguishable (identical actually).

i) Pick an input $x \in D$ at random, and output $(x, f(x))$.

ii) Pick an output $y \in R$ at random, and output $(f^{-1}(x), y)$.

Denote this property $\mathbb{P}$.

2.2 Instantiations

Notice that the RSA function $f(x) := x^e \pmod N, f^{-1}(y) := y^d \pmod N$ gives a trapdoor permutation and can be plugged into FDH directly. In the post-quantum setting, it is possible to instantiate the FDH approach using lattice and coding problems, but there are further technicalities to deal with.

Lattice-based FDH. Since SIS is surjective, it cannot be plugged into FDH directly. Gentry et al. [GPV08] observed that in the property $\mathbb{P}$, uniform distribution on the input is not essential. Instead a generalized property $\mathbb{P}'$ suffices for FDH. $\mathbb{P}'$ says that the following two distributions are identical (upto negligible error)

i) Pick $x \leftarrow D$ from some canonical distribution χ on D (not necessarily uniform), and output $(x, f(x))$.

ii) Pick $y \in_R R$ uniformly from the range, and sample a preimage $x \leftarrow_\chi \{f^{-1}(y)\}$. Output (x, y).

They formalized this idea in a notion called *preimage samplable functions*, and showed a construction based on the SIS problem where χ is a *discrete Gaussian* distribution.

Code-based FDH. Courtois et al. [CFS01] instantiatied FDH idea using the Syndrome decoding (SD) problem, which is probably the only unbroken signature code-based signature scheme. One difficulty was that the SD function $f_H(x) := Hx$ is injective. In particular the output y from $\mathcal{O}$ may not be decodable (i.e. outside the range of f_H). CFS addressed this by repeating, each time with a distinct counter, till a decodable y has been generated from $\mathcal{O}$. By setting proper parameters (n, k, d) and β, the resulting scheme remains practical. CFS gave informal justification of the scheme's security, and a formal proof only appeared much later in 2007 [Dal07]. The proof was based on two assumptions:

1. $H \leftarrow G(1^\lambda)$, sampled according to the procedure we descibed before, and $H' \in_R \mathbb{F}_2^{(n-k)\times n}$ a uniform random (parity check matrix) are compuationally indistinguishable.

2. $g_{H'}(x) := Hx$ for $x \in_R \mathbb{F}_2^n$ with $\|x\| \le \beta$ is hard to invert.

Note that the two assumptions together imply that g_H is also one-way and hence are stronger. However, in a recent work [FGUO+13], the first assumption was disproved under the parameter set for CFS signature. This leaves a provable security of CFS signature at question.

3 Public-key Encryption

Given a trapdoor function, a natural proposal for an public-key encryption scheme would be setting $pk := f, sk := f^{-1}$ and letting

$$\mathsf{Enc}(pk, m) := f(m); \quad \& \quad \mathsf{Dec}(sk, c) = f^{-1}(c).$$

The scheme using the RSA function is sometimes called the "text-book" RSA encryption. Other examples essentially fall into this category:

- **lattice-based**: some early proposals e.g., [GGH97]. NTRU [HPS98]?
- **code-based**: the two (equivalent) major proposals: **McEliece** [McE78] (using code-decoding CD function, see Lecture 1) and **Niederreiter** [Nie86] (using syndrome-decoding SD function, see Lecture 1).
- **MQ-based**: basically all proposals, e.g. Matsumoto&Imai [MI88] and Patarin's Hidden Field Equation (HFE) [Pat96].

However the resulting schemes only ensures very weak security[2]. To get standard security notions for PKE, we need more sophisticated constructions.

Recall two standard security notions for PKE

- IND-CPA (indistinguishable encryptions under chosen-*plaintext*-attacks): roughly, given ciphertexts that encrypt either 0 or 1, and any adversary (implicitly having access to an encrytion oracle since pk is public) cannot distinguish the two cases.
- IND-CCA (indistinguishable encryptions under chosen-*ciphertext*-attacks): roughly, we require the same distinguishing task above being hard for any adversay, but the adversary is additionally given access to a decryption oracle, with the only constraint that the decrypting query cannot be the received ciphertext. Two variants: CCA1 and CCA2. Our future discussion refers to CCA2.

[2]This might be OK for typical use cases, where PKE is used as a *Key-encapsulation Mechanism* (KEM) to trasfer a randomly genreated key for a symmetric encryption scheme.

3.1 Achieving CPA- & CCA security in RO

Bellare-Rogaway CPA & CCA. In the seminal paper by Bellare and Rogaway [BR93], they formalized the random-oracle model and (among other results) proposed constructions of IND-CPA and IND-CCA (with an additional *symmetric* IND-CCA encryption) PKE in RO from any trapdoor one-way permutations.

We only discuss their IND-CPA construction in Fig. 1. Let (f, f^{-1}) be a trapdoor one-way permutation. Intuitively, as long as f is hard to invert, y would be totally random which acts as a one-time-pad on plaintext m.

KeyGen $G(1^\lambda)$:	**Encrypt** $\mathsf{Enc}(m, pk)$:	**Decrypt** $\mathsf{Dec}(sk, c)$:
$pk := f, sk := f^{-1}$.	• $r \in_R \{0,1\}^k$. Get $y := \mathcal{O}(r)$, • Output $c := (f(r), y \oplus m)$.	• Parse c as (c_1, c_2). • Compute $r \leftarrow f^{-1}(c_1)$ and output $m := c_2 \oplus \mathcal{O}(r)$.

Figure 1: IND-CPA PKE in RO from trapdoor permutations [BR93]

Efficiency improvement: OAEP & OAEP+. One shortcoming of the constructions above is the efficiency overhead (e.g. longer ciphertexts). Bellare and Rogaway proposed another transformation - *optimal asymmetric encryption padding* (OAEP) based on any trapdoor permutations, which they claimed to achieved IND-CCA. However, a bug in their proof was later identified, and only IND-CPA (& IND-CCA-1) can be achieved. Nonetheless OAEP with the RSA permutation is indeed IND-CCA as shown by [Sho01, FOPS04], and RSA-OAEP was subsequently standardized in PKCS#1 v2[3]. [FOPS04] actually showed that any trapdoor permutation with the special *partially one-way* security property gives IND-CCA under OAEP. Shoup [Sho01] also gave a variant of OAEP called OAEP + which achieves IND-CCA with any trapdoor permutation (standard one-way).

We review OAEP here which employs the powerful Feistel network. We need

- (f, f^{-1}): a trapdoor permutation on $\{0,1\}^{n+k_0+k_1}$.
- $\mathcal{O}_1 : \{0,1\}^{k_0} \to \{0,1\}^{n+k_1}$: random oracle 1.
- $\mathcal{O}_2 : \{0,1\}^{n+k_1} \to \{0,1\}^{k_0}$: random oracle 2.

KeyGen $G(1^\lambda)$:	**Encrypt** $\mathsf{Enc}(pk, m)$:	**Decrypt** $\mathsf{Dec}(sk, c)$:
$pk := f, sk := f^{-1}$.	• Sample $r \in_R \{0,1\}^{k_0}$. $m' := m\|\bar{0}$ denotes message m appended with k_1 bits of 0. • Compute $s := \mathcal{O}_1(r) \oplus m'$, and $t := \mathcal{O}_2(s) \oplus r$. • Output $c := f(s\|t)$.	• Compute $f^{-1}(c)$ and parse it as $s\|t$. • Compute $r := \mathcal{O}_2(s) \oplus t$ and $m' := \mathcal{O}_1(r) \oplus s$. Output the first n bits of m' as m.

Figure 2: IND-CPA from OAEP [BR94]

Remark 1. Most (if not all) of these transformations should also work with *injective* trapdoor functions. [Exercise: check if this is true.]

[3] `https://tools.ietf.org/html/rfc2437`.

Other generic conversions in RO from weaker assumptions. Another aspect of improving the constructions above is to use weaker primitives (such as IND-CPA PKE) as opposed to injective trapdoor one-way functions. There are quite a few generic constructions in RO with various flavors, see [FO99, Poi00, OP01, FO13]. An interesting question would be to figure out if we can instantiate these constructions based on post-quantum problems. As an example, [KI01] showed how to convert McEliece PKE to IND-CCA by the transformaitons of Fujisaki-Okamoto transformation [FO99], Pointcheval [Poi00], and a more efficient variant of these two.

3.2 Direct CPA- & CCA-secure constructions

[Reading]

Lattice-based PKE. Regev's PKE based on LWE [Reg09], achieves IND-CPA. The essence of the proof is a *leftover hash lemma*. A dual version was proposed in [GPV08].

KeyGen $G(1^\lambda)$:	**Encrypt** $\mathsf{Enc}(pk, m), m \in \{0,1\}$:	**Decrypt** $\mathsf{Dec}(sk, c)$:
• Sample $A \in_R \mathbb{Z}_q^{m\times n}$, $s \in_R \mathbb{Z}_q^n$ and $e \leftarrow \chi^m$. • Output $pk := (A, b := As + e), sk := s$.	• Sample $r \in_R \{0,1\}^m$. Compute $p := r^T A$ and $u := r^T b + m \cdot \lfloor q/2 \rceil$. • Output $c := (p, u)$.	• Parse c as (p, u) and compute $z := u - p \cdot s$. • Output 0 if z is closer to 0 and output 1 if z is closer to $\lfloor \frac{q}{2} \rceil$.

Figure 3: Regev's IND-CPA PKE from LWE

Observe that decryption is correct with high probability because

$$u - ps = r^T(As + e) + m \cdot \lfloor \frac{q}{2} \rceil - r^T As = r^T e + m \cdot \lfloor \frac{q}{2} \rceil \approx m \cdot \lfloor \frac{q}{2} \rceil \pmod q .$$

Approximation holds because $r^T e$ is of small norm.

Peikert & Waters [PW11] introduced the notion of *lossy trapdoor functions* and constructed (the first) IND-CCA PKE in the plain model (i.e., without RO) based on LWE. Soon after, Peikert [Pei09] gave a simpler construction based on the injective trapdoor function from LWE we discussed earlier.

Code-based PKE. Nojima et al. [NIKM08] showed that the McEliece cryptosystem with a random padding (roughly encrypting $r \| m$ with random r, which may not be secure in general) achieves IND-CPA. Döttling et al. [DDMQN12] constructed a variant of McElice based on ideas of [RS10] that realizes IND-CCA. Based on the *learning with parity* (LPN) problem, Alekhnovich [Ale03] proposed a IND-CPA encryption scheme. LPN is essentially the code decoding problem CD where the Generating matrix is uniformly random. It can be viewed as a special case of LWE as well.

(Incomplete) summary: PQ-Enc schemes

Approach	Security	Instantiation		
		Lattice	**Code**	**MQ**
"Text-book" RSA. w. trapdoor functions	one-way?	• [GGH97] • NTRU [HPS98]?	McEliece [McE78], Niederreiter [Nie86]	[MI88, Pat96] ...
Constructions in random-oracle model (RO)				
[BR93] hybrid	IND-CPA in **RO**	applicable		
[BR93] with CCA Symmetric Enc	IND-CCA in **RO**	applicable		
OAEP [BR94]	≥ IND-CPA in **RO**	applicable? can we get IND-CCA?		
OAEP+ [Sho01]	IND-CCA in **RO**	applicable?		
Other transformations [Poi00, FO99, OP01]...	IND-CCA in **RO**	KEM [Pei14]	[KI01]	applicable?
Direct constructions in plain model				
Ex. leftover hash lemma [HILL99]	IND-CPA	[Reg09, GPV08] ...	[Ale03, NIKM08]	?
"lossy" trapdoor functions & correlated products	IND-CCA	[PW11, Pei09, MP12] ...	[DDMQN12]	?

References

[Ajt99] Miklós Ajtai. Generating hard instances of the short basis problem. In *Automata, Languages and Programming*, pages 1–9. Springer, 1999.

[Ale03] Michael Alekhnovich. More on average case vs approximation complexity. In *Foundations of Computer Science, 2003. Proceedings. 44th Annual IEEE Symposium on*, pages 298–307. IEEE, 2003.

[AP11] Joël Alwen and Chris Peikert. Generating shorter bases for hard random lattices. *Theory of Computing Systems*, 48(3):535–553, 2011. Preliminary version in STACS 2009.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM conference on Computer and communications security*, pages 62–73. ACM, 1993.

[BR94] Mihir Bellare and Phillip Rogaway. Optimal asymmetric encryption. In *Advances in Cryptology—EUROCRYPT'94*, pages 92–111. Springer, 1994.

[BR96] Mihir Bellare and Phillip Rogaway. The exact security of digital signatures-how to sign with rsa and rabin. In *Advances in Cryptology—Eurocrypt'96*, pages 399–416. Springer, 1996.

[CFS01] Nicolas T Courtois, Matthieu Finiasz, and Nicolas Sendrier. How to achieve a McEliece-based digital signature scheme. In *Advances in Cryptology—ASIACRYPT 2001*, pages 157–174. Springer, 2001.

[CGH04] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. *Journal of the ACM (JACM)*, 51(4):557–594, 2004.

[CHKP12] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. *Journal of cryptology*, 25(4):601–639, 2012. Preliminary version in Eurocrypt 2010.

[Dal07] Léonard Dallot. Towards a concrete security proof of courtois, finiasz and sendrier signature scheme. In *Research in Cryptology*, pages 65–77. Springer, 2007.

[DDMQN12] Nico Döttling, Rafael Dowsley, Jörn Müller-Quade, and Anderson CA Nascimento. A cca2 secure variant of the McEliece cryptosystem. *Information Theory, IEEE Transactions on*, 58(10):6672–6680, 2012. Preliminary version in CT-RSA 2009.

[DN12] Léo Ducas and Phong Q Nguyen. Learning a zonotope and more: Cryptanalysis of ntrusign countermeasures. In *Advances in Cryptology–ASIACRYPT 2012*, pages 433–450. Springer, 2012.

[FGUO+13] Jean-Charles Faugere, Valérie Gauthier-Umana, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. A distinguisher for high-rate McEliece cryptosystems. *Information Theory, IEEE Transactions on*, 59(10):6830–6844, 2013.

[FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *Advances in Cryptology - CRYPTO '99*, pages 537–554, 1999. Full version in Journal of cryptology 2013.

[FO13] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. *Journal of cryptology*, 26(1):80–101, 2013. Preliminary version in Crypto'99.

[FOPS04] Eiichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval, and Jacques Stern. Rsa-oaep is secure under the rsa assumption. *Journal of Cryptology*, 17(2):81–104, 2004. Prelim in Crypto'01.

[GGH97] Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Public-key cryptosystems from lattice reduction problems. In *Advances in Cryptology—CRYPTO'97*, pages 112–131. Springer, 1997.

[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*, pages 197–206. ACM, 2008.

[GS02] Craig Gentry and Mike Szydlo. Cryptanalysis of the revised ntru signature scheme. In *Advances in Cryptology—EUROCRYPT 2002*, pages 299–320. Springer, 2002.

[HHGP+03] Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H Silverman, and William Whyte. Ntrusign: Digital signatures using the ntru lattice. In *Topics in cryptology—CT-RSA 2003*, pages 122–140. Springer, 2003.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999.

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. Ntru: A ring-based public key cryptosystem. In *Algorithmic number theory*, pages 267–288. Springer, 1998.

[HPS01] Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. Nss: An ntru lattice-based signature scheme. In *Advances in Cryptology—Eurocrypt 2001*, pages 211–228. Springer, 2001.

[KI01] Kazukuni Kobara and Hideki Imai. Semantically secure McEliece public-key cryptosystems-conversions for mceliece pkc. In *Public Key Cryptography*, pages 19–35. Springer, 2001.

[McE78] RJ McEliece. A public-key cryptosystem based on algebraic coding theory. *The Deep Space Network Progress Report*, 42(44):114–116, 1978.

[MI88] Tsutomu Matsumoto and Hideki Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Advances in Cryptology—EUROCRYPT'88*, pages 419–453. Springer, 1988.

[MP12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Advances in Cryptology–EUROCRYPT 2012*, pages 700–718. Springer, 2012.

[Nie86] Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15:19–34, 1986. Problemy Upravlenija i Teorii Informacii 15, 159–166.

[NIKM08] Ryo Nojima, Hideki Imai, Kazukuni Kobara, and Kirill Morozov. Semantic security for the mceliece cryptosystem without random oracles. *Designs, Codes and Cryptography*, 49(1-3):289–305, 2008.

[NR09] Phong Q Nguyen and Oded Regev. Learning a parallelepiped: Cryptanalysis of ggh and ntru signatures. *Journal of Cryptology*, 22(2):139–160, 2009. Preliminary version in Eurocrypt 2006.

[OP01] Tatsuaki Okamoto and David Pointcheval. REACT: Rapid enhanced-security asymmetric cryptosystem transform. In *Topics in Cryptology—CT-RSA 2001*, pages 159–174. Springer, 2001.

[Pat96] Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (ip): Two new families of asymmetric algorithms. In *Advances in Cryptology—EUROCRYPT'96*, pages 33–48. Springer, 1996.

[Pei09] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 333–342. ACM, 2009.

[Pei14] Chris Peikert. Lattice cryptography for the internet. In *Post-Quantum Cryptography*, pages 197–219. Springer, 2014.

[Poi00] David Pointcheval. Chosen-ciphertext security for any one-way cryptosystem. In *Public Key Cryptography*, pages 129–146. Springer, 2000.

[PW11] Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. *SIAM Journal on Computing*, 40(6):1803–1844, 2011. Preliminary version in STOC 2008.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):34, 2009.

[RS10] Alon Rosen and Gil Segev. Chosen-ciphertext security via correlated products. *SIAM Journal on Computing*, 39(7):3058–3088, 2010. Preliminary version in STOC 2009.

[Sho01] Victor Shoup. Oaep reconsidered. In *Advances in Cryptology—CRYPTO 2001*, pages 239–259. Springer, 2001.