Game-Based Security Proofs

A chronological reading list

Companion to `all-uc-papers.pdf`. That list walks the universally-composable literature and, under each paper, names the ideal functionalities it introduces or uses. This one walks the *game-based* literature and, under each paper, names the games, lemmas and transformations it introduces.

These are *representative* papers, not all of them. A paper earns a place here if it states a security notion as a formal game and proves something formally about it — and if reading it in sequence with the others shows how the style got from one place to the next. It starts in 1982, with the first security definition written as an experiment between an adversary and a challenger, and ends with proofs of deployed protocols that no single game sequence could hold. Full bibliographic data, with DOI and ePrint links, is in the References at the end.

Each entry is tagged:

- [DEFN] states a new security notion as a formal game;
- [METHOD] a proof technique or framework for chaining games;
- [TOOL] mechanizes that methodology (computer-aided / machine-checked);
- [TURN] a turning point — a proof that broke or a definition shown inadequate, which changed how games were written afterwards;
- [CASE] a landmark formal proof of a real primitive or protocol.

If you read only five. [GM82] (where the experiment comes from); [BDJR97] (what a fully formal, concrete game-based treatment of one primitive looks like); [Sho04] and [BR04] (the method itself, in prose and in a formal system); and [BDLF+18] (how it is done at protocol scale today).

1982 — the experiment appears

1. [DEFN] Goldwasser & Micali, *Probabilistic Encryption & How to Play Mental Poker Keeping Secret All Partial Information* [GM82, GM84].
   a. **Polynomial security**: the adversary names two messages, receives an encryption of one of them, and must say which — the first security definition phrased as an *experiment* between a challenger and an adversary. Renamed IND-CPA later.
   b. **Semantic security**: whatever is efficiently computable about the plaintext from the ciphertext is computable without it.
   c. The proof that the two are equivalent is arguably the first **game hop** in the literature: a security experiment rewritten step by step into a different one.
   d. The **hybrid argument**, used to go from single-bit to multi-bit messages. Every later multi-step game chain is this argument generalized.
2. [DEFN] Yao, *Theory and Application of Trapdoor Functions* [Yao82].
   a. **Computational indistinguishability** of distribution ensembles: the relation that every "these two games are close" step is ultimately an instance of.
   b. Next-bit unpredictability $\iff$ indistinguishability (with [BM84]) — an early proof that two differently-shaped games define the same thing.

3. [DEFN] Blum & Micali, *How to Generate Cryptographically Strong Sequences of Pseudorandom Bits* [BM84].
    a. The **next-bit test**: a *prediction* game rather than a distinguishing game. The two shapes — guess a hidden bit vs. produce a winning object — are still the only two shapes in use.

1984 — oracles enter the game

1. [DEFN] Goldreich, Goldwasser & Micali, *How to Construct Random Functions* [GGM84].
    a. **PRF game**: distinguish oracle access to $F_k(\cdot)$ from oracle access to a uniformly random function. The first widely-used game in which the adversary *queries an oracle adaptively* rather than receiving a fixed challenge.
    b. The GGM tree's analysis is the canonical multi-hop chain: one hybrid per level, each neighboring pair indistinguishable by the PRG game.
2. [DEFN] Goldwasser, Micali & Rivest, *A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks* [GMR88].
    a. **EUF-CMA**: the adversary gets a signing oracle and wins by forging on any message it did not query. The template for every "win condition + oracle" game since.
    b. The **attack/break taxonomy** — key-only, known-message, generic and adaptive chosen-message attacks, crossed with total break, universal/selective/existential forgery — the first systematic grid of games for a single primitive.

1985 — the road forks

1. [TURN] Goldwasser, Micali & Rackoff, *The Knowledge Complexity of Interactive Proof Systems* [GMR89].
    a. Zero knowledge is defined by exhibiting a **simulator**, not by bounding an adversary's advantage in a game. This is the branch that leads to UC [Can01] and to `all-uc-papers.pdf`.
    b. Included as the fork in the road: read next to [GM82] to watch the two proof styles separate. Everything below is the game branch.

1988

1. [DEFN] [METHOD] Luby & Rackoff, *How to Construct Pseudorandom Permutations from Pseudorandom Functions* [LR88].
    a. **PRP game** and **strong-PRP game** (the latter also gives the adversary the inverse oracle).
    b. The Feistel analysis proceeds through a sequence of idealized experiments, bounding the probability of a collision event that makes them differ — game playing with a bad event, about fifteen years before it was named in [BR04].

1990–1991 — the CCA ladder

1. [DEFN] Naor & Yung, *Public-Key Cryptosystems Provably Secure Against Chosen Ciphertext Attacks* [NY90].
    a. **IND-CCA1** ("lunchtime"): a decryption oracle, available only *before* the challenge ciphertext is handed over.

2. [DEFN] Rackoff & Simon, *Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack* [RS91].
    a. **IND-CCA2**: the decryption oracle stays available after the challenge, with the challenge ciphertext itself excluded. That exclusion clause is the single most-revisited line in any security game — see [BHK09].
3. [DEFN] Dolev, Dwork & Naor, *Non-Malleable Cryptography* [DDN91].
    a. **NM-CPA / NM-CCA**, defined by comparing the real adversary against a simulator that never sees the ciphertext — a definition deliberately straddling the game and simulation styles, later also given a purely game-based (comparison-free) form.

1993 — concrete security, and the first protocol games

1. [DEFN] [METHOD] Bellare & Rogaway, *Random Oracles are Practical: A Paradigm for Designing Efficient Protocols* [BR93b].
    a. The **random oracle model**: the hash function becomes an oracle *inside* the game, which the reduction may observe and program. Hugely enabling — and the source of most later disputes about what a game-based theorem means ([CGH04], [BHK13]).
    b. **Concrete security**: theorems stated as explicit (t, q, ϵ) relations rather than asymptotics, which is what makes a game's advantage function the deliverable.
2. [DEFN] Bellare & Rogaway, *Entity Authentication and Key Distribution* [BR93a].
    a. The **BR key-exchange game**: sessions modeled as oracles $\Pi^s_{i,j}$, with **Send**, **Reveal** and **Corrupt** queries, plus a single **Test** query answered with either the real session key or a random one.
    b. **Matching conversations** as the partnering predicate — the bookkeeping that says which sessions are supposed to share a key.
    c. Directly ancestral to [CK01], [JKSS12] and [FG14]. If you want to see where protocol security games come from, this is the paper.

1994–1997 — the concrete-security school

1. [METHOD] [CASE] Bellare, Kilian & Rogaway, *The Security of Cipher Block Chaining* [BKR94].
    a. PRF-security of CBC-MAC with an explicit birthday bound ($\approx q^2\ell^2/2^n$): the first influential proof whose *point* is the shape of the advantage function, not merely that it is negligible.
2. [DEFN] [TURN] Bellare & Rogaway, *Optimal Asymmetric Encryption* [BR94].
    a. **Plaintext awareness**: an adversary that produces a valid ciphertext must "know" the plaintext, formalized via an extractor reading its random-oracle queries.
    b. The claimed IND-CCA2 implication is the famous one that did not hold — see [Sho01].
3. [DEFN] [CASE] Bellare, Canetti & Krawczyk, *Keying Hash Functions for Message Authentication* [BCK96].
    a. MAC security as a formal game, and the reduction of HMAC to two assumptions on the compression function (PRF-ness, weak collision resistance) — rather than to an unanalyzed "hash is good" wish.
    b. The paper that made the whole concrete-security style credible to practitioners, because the object it analyzed shipped everywhere.

4. [METHOD] Kilian & Rogaway, *How to Protect DES Against Exhaustive Key Search* [KR96].
    a. A proof built as a sequence of games that are **identical until a flag is set**, with the whole difference charged to that flag. [BR04] points at this paper as where their framework came from.
5. [METHOD] Pointcheval & Stern, *Security Proofs for Signature Schemes* [PS96].
    a. The **forking lemma**: run the adversary twice on the same random tape with divergent oracle answers. Rewinding as a reusable game transformation; generalized in [BN06].
    b. The **splitting lemma**, the probability bookkeeping that makes the forking argument go through.
6. [METHOD] Bellare & Rogaway, *The Exact Security of Digital Signatures — How to Sign with RSA and Rabin* [BR96].
    a. **Tightness** promoted to a design goal: the scheme is chosen so that the game hop loses as little as possible. Sharpened in [Cor00], bounded from below in [BJLS16].
7. [DEFN] Bellare, Desai, Jokipii & Rogaway, *A Concrete Security Treatment of Symmetric Encryption* [BDJR97].
    a. Four formalizations of chosen-plaintext security — **find-then-guess**, **left-or-right**, **real-or-random** and **semantic** — each a precisely written game, with the reductions between them and their exact advantage losses.
    b. Concrete PRF-based analyses of ECB, CBC, CTR and friends in one common framework.
    c. The single best specimen of what a complete, formal, game-based treatment of one primitive looks like; still the template modern papers copy.
8. [DEFN] [METHOD] Shoup, *Lower Bounds for Discrete Logarithms and Related Problems* [Sho97].
    a. The **generic group model**: group elements become opaque handles served by an oracle, so an adversary's whole interaction is a game the analysis can control.
    b. Lower bounds proved by exactly the bad-event argument later formalized in [BR04] — two group elements' encodings collide.

1998 — mapping the space of games

1. [METHOD] Bellare, *Practice-Oriented Provable-Security* [Bel98].
    a. The manifesto for the style the rest of this list assumes: explicit games, explicit reductions, explicit constants. Short; read it first if you want the philosophy before the mathematics.
2. [DEFN] Bellare, Desai, Pointcheval & Rogaway, *Relations Among Notions of Security for Public-Key Encryption Schemes* [BDPR98].
    a. The $\{\mathrm{IND}, \mathrm{NM}\} \times \{\mathrm{CPA}, \mathrm{CCA1}, \mathrm{CCA2}\}$ lattice: every implication proved by a game transformation, every non-implication by a separating counterexample.
    b. Establishes the genre of "relations among notions" papers — papers whose entire content is the formal relationship between games.
3. [TURN] Canetti, Goldreich & Halevi, *The Random Oracle Methodology, Revisited* [CGH04].
    a. A scheme provably secure in the random-oracle game and insecure for *every* concrete instantiation of the oracle. The first hard limit on what winning a ROM game buys you; made concrete for a natural scheme in [BBP03].

4. [CASE] Cramer & Shoup, *A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack* [CS98].

    a. First efficient IND-CCA2 scheme in the standard model; the proof is organized as a sequence of experiments with one explicit bad event (the simulator wrongly rejecting a ciphertext). Shoup's house style, six years before he wrote the method down in [Sho04].

2000 — more users, more oracles

1. [DEFN] Bellare, Boldyreva & Micali, *Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements* [BBM00].

    a. **Multi-user IND-CPA/CCA**: many keys, many challenges, one game. The generic hybrid costs a factor of $n \cdot q_e$; the paper identifies when you can avoid paying it. Sixteen years later this decides a standard — see [BT16].

2. [DEFN] Bellare & Namprempre, *Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm* [BN00].

    a. **INT-PTXT** and **INT-CTXT** games, crossed with IND-CPA/CCA.

    b. The verdict on Encrypt-and-MAC / MAC-then-Encrypt / Encrypt-then-MAC, each settled by a game argument or a counterexample. A definitional paper that changed what implementations do.

3. [METHOD] Coron, *On the Exact Security of Full Domain Hash* [Cor00].

    a. A sharper reduction for FDH: the security loss drops from the number of *hash* queries q_h (as in [BR96]) to the number of *signature* queries q_s, orders of magnitude smaller in practice.

    b. A **meta-reduction** showing the remaining q_s loss cannot be removed by any reduction of that shape — the technique behind every tightness lower bound in this list.

4. [DEFN] Bellare, Pointcheval & Rogaway, *Authenticated Key Exchange Secure against Dictionary Attacks* [BPR00].

    a. The **PAKE game**: [BR93a] plus a small password dictionary, where the adversary's advantage must be bounded by its number of *online* guesses rather than made negligible. A game whose *shape* had to change to match the primitive.

2001 — a famous proof breaks

1. [TURN] Shoup, *OAEP Reconsidered* [Sho01].

    a. The proof in [BR94] is *wrong*: plaintext awareness does not yield IND-CCA2 for a general one-way trapdoor function. One game hop did not hold.

    b. The most-cited cautionary tale in the field, and the strongest argument for writing proofs as checkable game sequences — and, eventually, for machine-checking them [BGB09].

2. [CASE] Fujisaki, Okamoto, Pointcheval & Stern, *RSA-OAEP is Secure under the RSA Assumption* [FOPS04].

    a. The repair: a valid but much lossier chain, exploiting RSA's specific structure rather than generic one-wayness.

3. [DEFN] [CASE] Boneh & Franklin, *Identity-Based Encryption from the Weil Pairing* [BF03].

a. **IND-ID-CCA**: the IND-CCA game extended with an adaptive *key-extraction* oracle for identities other than the challenge one. A clean example of adding one oracle to an existing game to define a new primitive.

b. The proof is a textbook ROM game chain, and it is what made a whole decade of pairing-based definitions follow the same recipe.

4. [DEFN] [METHOD] Canetti & Krawczyk, *Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels* [CK01].

   a. The **CK model**: a game-based key-exchange definition packaged with a modular composition theorem (authenticators / the AM-to-UM compiler).

   b. The clearest early attempt to get composition — UC's selling point — while staying inside a game.

5. Canetti, *Universally Composable Security: A New Paradigm for Cryptographic Protocols* [Can01].

   a. Listed only as the pointer to the other document: from here on the simulation branch is tracked in `all-uc-papers.pdf`. Much of the game-side work below is a response to what UC offers and games do not — composition.

2002–2003 — new primitives get formal games

1. [METHOD] Maurer, *Indistinguishability of Random Systems* [Mau02].

   a. **Random systems** and **monotone conditions**: an abstract, code-free alternative to game playing, where "identical-until-bad" becomes conditional equivalence of two systems.

   b. Reaches the same bounds as code-based games by a different route; worth reading precisely because it is the road not taken. See also [MPR07].

2. [DEFN] Rogaway, *Authenticated-Encryption with Associated-Data* [Rog02].

   a. The **AEAD game**, nonce-based: privacy and authenticity of a message plus unencrypted-but-authenticated headers. The game essentially every deployed cipher suite is now proved against.

3. [METHOD] [CASE] Cramer & Shoup, *Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack* [CS03].

   a. Hash proof systems, and a long proof written as an explicit, numbered sequence of games — the immediate precursor to [Sho04].

4. [DEFN] Bellare, Micciancio & Warinschi, *Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions* [BMW03].

   a. **Full-anonymity** and **full-traceability**: two games that provably subsume the dozen informal requirements the group signature literature had accumulated.

   b. The clearest demonstration of what formalizing as games buys you: a folklore list of properties collapses to two definitions, and the collapse is a theorem. Compare [BSZ05] for the dynamic case.

5. [DEFN] Bellare, Namprempre, Pointcheval & Semanko, *The One-More-RSA-Inversion Problems and the Security of Chaum's Blind Signature Scheme* [BNPS03].

   a. **One-more-RSA-inversion**: a new *assumption* stated as a game (invert $n+1$ targets given n oracle inversions), because no standard assumption could support the proof.

   b. **Blindness** and **one-more-unforgeability** for blind signatures. Shows the move of pushing the interactive difficulty out of the proof and into a formally-stated game assumption — now routine.

2004 — the year games were formalized

1. [METHOD] Shoup, *Sequences of Games: A Tool for Taming Complexity in Security Proofs* [Sho04].
   a. **Transitions based on indistinguishability**: replace a distribution with a computationally close one; the hop costs one assumption.
   b. **Transitions based on failure events**, justified by the **Difference Lemma**: if G_i and G_{i+1} proceed identically unless event F occurs, then $|\Pr[S_i] - \Pr[S_{i+1}]| \leq \Pr[F]$.
   c. **Bridging steps**: purely syntactic rewrites that change nothing but make the next real step visible. Naming these is half the contribution — they are where informal proofs hide their mistakes.
   d. Worked end-to-end examples: hashed ElGamal, Cramer–Shoup, PSS.

2. [METHOD] Bellare & Rogaway, *Code-Based Game-Playing Proofs and the Security of Triple Encryption* [BR04, BR06].
   a. **Games as pseudocode**: a game is a program with `Initialize`, oracle procedures and `Finalize`; the adversary is linked against it. Proof steps become *program* rewrites, which is what later makes mechanization possible.
   b. The **bad flag** discipline: games are written to be syntactically **identical-until-bad**.
   c. The **Fundamental Lemma of game playing**: if G and H are identical-until-bad, then $|\Pr[G^A \Rightarrow 1] - \Pr[H^A \Rightarrow 1]| \leq \Pr[G^A \text{ sets } \mathsf{bad}]$.
   d. **Lazy vs. eager sampling**, coin-fixing and resampling: the standard library of bridging rewrites, each proved once.
   e. Application: triple encryption's $\approx 2^{78}$ security bound.
   f. This and [Sho04] are the two documents the phrase "game-based proof" refers to. Read both: Shoup's is the prose method, this one is the formal system.

3. [DEFN] [METHOD] Maurer, Renner & Holenstein, *Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology* [MRH04].
   a. The **indifferentiability** game, plus the composition theorem that ordinary game-based definitions lack: a construction indifferentiable from a random oracle can replace one in any single-stage game.
   b. The standard tool for hash-function domain extension (Merkle–Damgård, sponges) — and, later, a cautionary tale of its own [RSS11].

4. [DEFN] Rogaway & Shrimpton, *Cryptographic Hash-Function Basics* [RS04].
   a. Seven games for hash functions — **Coll**, **Pre**, **ePre**, **aPre**, **Sec**, **eSec**, **aSec** — with the complete implication/separation map between them.
   b. A model of definitional hygiene: the differences between these games are exactly the differences practitioners get wrong.

5. [DEFN] Rogaway, *Nonce-Based Symmetric Encryption* [Rog04].
   a. Replaces the random IV of [BDJR97] with a **nonce** the adversary picks (subject to non-repetition), which is what real APIs expose.
   b. Read as a pair with [BDJR97]: the same primitive, re-formalized a second time because the first game's interface did not match how the primitive is used.

2005–2007 — mechanize it, and keep defining

1. [TOOL] Halevi, *A Plausible Approach to Computer-Aided Cryptographic Proofs* [Hal05].
   a. The founding document of computer-aided game-based cryptography: since a game sequence is a sequence of *program* rewrites, a tool should check them.
   b. Proposes exactly the architecture — a game-transformation engine plus a proof checker — that [Bla06], [BGB09] and [BGHB11] went on to build.
2. [TOOL] Blanchet, *A Computationally Sound Mechanized Prover for Security Protocols* [Bla06].
   a. First tool to *find* game sequences automatically in the computational model (as opposed to the symbolic/Dolev–Yao model).
   b. Games as processes; hops as observational-equivalence-preserving process rewrites.
3. [DEFN] Rogaway & Shrimpton, *A Provable-Security Treatment of the Key-Wrap Problem* [RS06].
   a. **Deterministic authenticated encryption (DAE)**: a game for a primitive that had shipped for years (key wrapping) with no definition at all.
   b. The cleanest case study in reverse-engineering a formal game from deployed practice, rather than designing practice to fit a game.
4. [DEFN] [TURN] Rogaway, *Formalizing Human Ignorance: Collision-Resistant Hashing without the Keys* [Rog06].
   a. Why there is no sensible collision-resistance *game* for a fixed, unkeyed hash like SHA-256 — a collision exists, so some adversary has it hardwired.
   b. The **explicit-reduction** workaround: state theorems as constructive transformations of adversaries rather than as advantage inequalities. A rare case of the game formalism being replaced rather than patched.
5. [METHOD] Bellare & Neven, *Multi-Signatures in the Plain Public-Key Model and a General Forking Lemma* [BN06].
   a. The **general forking lemma**: [PS96]'s forking stated as a self-contained probabilistic lemma about algorithms, decoupled from signatures, so it can be dropped into any game chain.
6. [DEFN] Bellare, Boldyreva & O'Neill, *Deterministic and Efficiently Searchable Encryption* [BBO07].
   a. **PRIV**: the best achievable privacy game once encryption must be deterministic — security only for messages of high min-entropy, which requires the game to quantify over message distributions rather than message pairs.
   b. Shows how to write a formal game for a primitive that cannot meet the standard one, instead of declaring it insecure and moving on. (It is also one of the multi-stage games [RSS11] later singles out.)
7. [METHOD] Maurer, Pietrzak & Renner, *Indistinguishability Amplification* [MPR07].
   a. Composing several "somewhat indistinguishable" systems into a very indistinguishable one: the amplification counterpart to the Fundamental Lemma, in [Mau02]'s random-systems framework.

2009–2012 — machine checking, and definitional hygiene

1. [TOOL] Barthe, Grégoire & Zanella Béguelin, *Formal Certification of Code-Based Cryptographic Proofs* [BGB09].

a. [BR04]'s code-based games formalized in Coq: a game is a program in a probabilistic imperative language, a hop is a certified program transformation.

b. **Probabilistic relational Hoare logic (pRHL)**, the logic in which "these two games behave identically unless bad" becomes a checkable judgment. Still the technical core of EasyCrypt today.

c. First fully machine-checked proofs of OAEP and of the Fundamental Lemma itself.

2. [TURN] [DEFN] Bellare, Hofheinz & Kiltz, *Subtleties in the Definition of IND-CCA: When and How Should Challenge-Decryption be Disallowed?* [BHK09].

   a. Four different formalizations of "the adversary may not decrypt the challenge" that the literature had treated as interchangeable, with separations showing they are not.

   b. The cleanest evidence that a game's small print is load-bearing.

3. [TOOL] Barthe, Grégoire, Heraud & Zanella Béguelin, *Computer-Aided Security Proofs for the Working Cryptographer* [BGHB11].

   a. [BGB09]'s ideas behind a proof assistant a cryptographer can actually drive: the game sequence is written in something close to the paper's own pseudocode, with SMT discharging the routine steps.

   b. The tool most current game-based mechanization is built on.

4. [DEFN] Boneh, Dagdelen, Fischlin, Lehmann, Schaffner & Zhandry, *Random Oracles in a Quantum World* [BDF+11].

   a. The **quantum random oracle model (QROM)**: the adversary queries the oracle in superposition, which invalidates the two moves every [BR93b] proof relies on — observing queries and programming answers.

   b. Re-proves classical results in the new game where possible, and separates where not. The starting point for essentially all post-quantum security proofs, including [HHK17].

5. [TURN] Ristenpart, Shacham & Shrimpton, *Careful with Composition: Limitations of Indifferentiability and Universal Composability* [RSS11].

   a. **Single-stage vs. multi-stage games**: [MRH04]'s composition theorem only applies to the former, and several important games (deterministic/hedged encryption, related-key attacks, proofs of storage) are multi-stage.

   b. The one composition theorem the game world had turns out to be narrower than everyone assumed — a direct motivation for [BDLF+18].

6. [DEFN] Bellare, Ristenpart & Tessaro, *Multi-Instance Security and its Application to Password-Based Cryptography* [BRT12].

   a. **m-out-of-n multi-instance games**: the adversary must break *all* m instances, which is the right question for password hashing and salting, and is not implied by single-instance security.

7. [DEFN] Bellare, Hoang & Rogaway, *Foundations of Garbled Circuits* [BHR12].

   a. Garbling promoted from a technique inside other protocols' proofs to a *primitive* with its own games: **privacy**, **obliviousness** and **authenticity**, in both indistinguishability and simulation flavors.

   b. The best example of the general move of this era: take something everyone proved ad hoc inside larger simulation arguments, give it standalone formal games, and let the rest of the literature reduce to them.

8. [DEFN] [CASE] Jager, Kohlar, Schäge & Schwenk, *On the Security of TLS-DHE in the Standard Model* [JKSS12].

a. The **ACCE game**: authenticated key exchange and stateful authenticated encryption fused into a single game, because TLS's handshake and record layer cannot be separated (the finished messages are encrypted under the key being established).
b. The canonical example of the game being reshaped to fit a deployed protocol rather than the reverse.

2013–2016 — new definitional idioms

1. [CASE] Krawczyk, Paterson & Wee, *On the Security of the TLS Protocol: A Systematic Analysis* [KPW13].
   a. Constrained-CCA / ACCE-style treatment covering TLS's actual ciphersuites, including RSA key transport.
2. [DEFN] Bellare, Hoang & Keelveedhi, *Instantiating Random Oracles via UCEs* [BHK13].
   a. **UCE (universal computational extractor)**: a family of standard-model games for hash functions, strong enough to replace the random oracle in many proofs, defined via a two-stage source/distinguisher game.
   b. The most ambitious attempt to answer [CGH04] with a definition rather than a disclaimer — and a good illustration of how delicate a new game is: several UCE variants were shown too strong soon after.
3. [DEFN] [CASE] Fischlin & Günther, *Multi-Stage Key Exchange and the Case of Google's QUIC Protocol* [FG14].
   a. The **multi-stage key-exchange game**: several keys per session, established at different times with different security levels, each testable. The model TLS 1.3 is analyzed in [DFGS21].
4. [TOOL] Petcher & Morrisett, *The Foundational Cryptography Framework* [PM15].
   a. Another Coq embedding of code-based games, aimed at extracting verified implementations alongside the proof.
5. [TURN] Bader, Jager, Li & Schäge, *On the Impossibility of Tight Cryptographic Reductions* [BJLS16].
   a. A general **meta-reduction** framework, in [Cor00]'s lineage: for a broad class of schemes with unique signatures/keys, *no* tight reduction from a non-interactive assumption exists.
   b. Turns tightness from a proof-quality question into a theorem about the game itself.
6. [DEFN] [CASE] Bellare & Tackmann, *The Multi-User Security of Authenticated Encryption: AES-GCM in TLS 1.3* [BT16].
   a. **Multi-user AE** with concrete bounds, applied to the exact nonce-randomization construction TLS 1.3 was choosing at the time.
   b. [BBM00]'s multi-user idea, sixteen years later, deciding a standard — a good closing argument for why the constants in a game matter.
7. Lindell, *How To Simulate It — A Tutorial on the Simulation Proof Technique* [Lin16].
   a. Not game-based — included as the companion tutorial for the other branch, and the fastest way to see which problems each style suits.

2017–2019 — modularity

1. [DEFN] [METHOD] Hofheinz, Hövelmanns & Kiltz, *A Modular Analysis of the Fujisaki–Okamoto Transformation* [HHK17].

a. The FO transform decomposed into small steps with a named game between each: IND-CPA → OW-PCVA → IND-CCA KEM, each hop proved separately and reusable.

b. The modern standard for how to write a reduction: modular, with explicit intermediate notions. Every NIST post-quantum KEM's proof is built out of these pieces.

2. [TOOL] Basin, Lochbihler & Sefidgar, *CryptHOL: Game-based Proofs in Higher-order Logic* [BLS17].

   a. Games as terms in Isabelle/HOL's probability monad, so game hops are equational rewriting rather than a bespoke program logic.

3. [METHOD] Brzuska, Delignat-Lavaud, Fournet, Kohbrok & Kohlweiss, *State Separation for Code-Based Game-Playing Proofs* [BDLF+18].

   a. **Packages**: games split into stateful components with disjoint state and typed interfaces, composed sequentially (∘) and in parallel (⊗).

   b. **Interchange / composition lemmas** letting a sub-package be replaced by an indistinguishable one *inside* a larger game — the modularity that UC had and plain game-based proofs did not.

   c. The main structural advance in game-based proving since [BR04], and what makes proofs of protocol-scale objects ([BDLE+22]) tractable.

4. [TURN] Drijvers, Edalatnejad, Ford, Kiltz, Loss, Neven & Stepanovs, *On the Security of Two-Round Multi-Signatures* [DEF+19].

   a. Several published two-round Schnorr multi-signature proofs are broken, by a concurrent (Wagner/ROS) attack their games' rewinding arguments could not see.

   b. The modern counterpart to [Sho01]: the reason the multi-signature literature now insists on fully formal games. See [NRS21] for the repair.

5. [TOOL] Canetti, Stoughton & Varia, *EasyUC: Using EasyCrypt to Mechanize Proofs of Universally Composable Security* [CSV19].

   a. The two branches meet in one tool: UC simulation proofs carried out in the game-based prover. Useful for seeing exactly where the styles differ formally.

2019–2021 — tooling consolidates

1. [TOOL] Barbosa, Barthe, Bhargavan, Blanchet, Cremers, Liao & Parno, *SoK: Computer-Aided Cryptography* [BBB+21].

   a. The survey to read before picking a tool: design-level (game-based) provers, symbolic provers, and verified implementations, with what each can and cannot do.

2. [TOOL] Haselwarter et al., *SSProve: A Foundational Framework for Modular Cryptographic Proofs in Coq* [HRM+21].

   a. [BDLF+18]'s state-separating proofs, mechanized: packages and their composition laws as a Coq library with a relational program logic underneath.

   b. Closes the loop [Hal05] opened in 2005 — modular *and* machine-checked.

3. [TOOL] Baelde, Delaune, Jacomme, Koutsos & Moreau, *An Interactive Prover for Protocol Verification in the Computational Model* [BDJ+21].

   a. A different bet: a logic for computational indistinguishability (after Bana–Comon) instead of explicit game rewriting.

4. [DEFN] [CASE] Nick, Ruffing & Seurin, *MuSig2: Simple Two-Round Schnorr Multi-Signatures* [NRS21].
    a. A two-round scheme with a full game-based proof that survives the attack of [DEF+19], in the ROM (plus a tighter argument in the algebraic group model).
    b. Worth reading immediately after [DEF+19]: the same game, one broken proof and one repaired one, a decade of technique apart.
5. [CASE] Dowling, Fischlin, Günther & Stebila, *A Cryptographic Analysis of the TLS 1.3 Handshake Protocol* [DFGS21].
    a. [FG14]'s full multi-stage game applied to the shipped TLS 1.3 handshake — and an example of a game-based analysis that shaped a standard while it was being written.

2022 and after — games at protocol scale

1. [CASE] [METHOD] Brzuska, Delignat-Lavaud, Egger, Fournet, Kohbrok & Kohlweiss, *Key-schedule Security for the TLS 1.3 Standard* [BDLE+22].
    a. [BDLF+18] applied at full scale: the TLS 1.3 key schedule proved as a composition of packages, at a size no monolithic game sequence would survive.
    b. The current answer to "can game-based proofs handle real protocols?" — yes, but only modularly.

Appendix: the standing critiques

Not definitional papers, but the arguments about what a game-based theorem actually claims. Useful once the rest of the list makes sense.

1. Koblitz & Menezes, *Another Look at "Provable Security"* [KM04]. Non-tight reductions read as meaningful, and the gap between a model's oracles and reality.
2. Bellare, Boldyreva & Palacio, *An Uninstantiable Random-Oracle-Model Scheme for a Hybrid Encryption Problem* [BBP03]. [CGH04]'s separation, for a natural scheme rather than a contrived one.
3. Dent, *Fundamental problems in provable security and cryptography* [Den06]. A survey of what the enterprise cannot deliver, written from inside it.
4. Bernstein & Lange, *Non-uniform Cracks in the Concrete: The Power of Free Precomputation* [BL13]. Adversaries with free preprocessing beat many concrete bounds as stated, so the quantifiers in a game matter as much as its shape.

The list in one line. Games were how definitions got written from 1982 [GM82], and how primitives got *fully* formalized from 1997 [BDJR97], but they were not themselves an object of study until 2004, when [Sho04] and [BR04] gave the sequence-of-games proof a grammar. What follows splits in two: mechanizing that grammar ([Hal05] → [Bla06] → [BGB09] → [BGHB11] → [BLS17, HRM+21]), and buying back the composability the style gave up when it declined to use simulators ([CK01] → [MRH04] → its limits in [RSS11] → state separation in [BDLF+18] → [BDLE+22]).

References

[BBB+21] Manuel Barbosa, Gilles Barthe, Karthik Bhargavan, Bruno Blanchet, Cas Cremers, Kevin Liao, and Bryan Parno. SoK: Computer-aided cryptography. Cryptology ePrint Archive, Paper 2019/1393, 2021. IEEE S&P '21.

[BBM00] Mihir Bellare, Alexandra Boldyreva, and Silvio Micali. Public-key encryption in a multi-user setting: Security proofs and improvements. In *EUROCRYPT '00*, pages 259–274, 2000.

[BBO07] Mihir Bellare, Alexandra Boldyreva, and Adam O'Neill. Deterministic and efficiently searchable encryption. In *CRYPTO '07*, pages 535–552, 2007.

[BBP03] Mihir Bellare, Alexandra Boldyreva, and Adriana Palacio. An uninstantiable random-oracle-model scheme for a hybrid encryption problem. Cryptology ePrint Archive, Paper 2003/077, 2003. EUROCRYPT '04.

[BCK96] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. Keying hash functions for message authentication. In *CRYPTO '96*, pages 1–15, 1996.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. Cryptology ePrint Archive, Paper 2010/428, 2011. ASIACRYPT '11.

[BDJ+21] David Baelde, Stéphanie Delaune, Charlie Jacomme, Adrien Koutsos, and Solène Moreau. An interactive prover for protocol verification in the computational model. In *IEEE S&P '21*, pages 537–554, 2021.

[BDJR97] Mihir Bellare, Anand Desai, E. Jokipii, and Phillip Rogaway. A concrete security treatment of symmetric encryption. In *FOCS '97*, pages 394–403, 1997.

[BDLE+22] Chris Brzuska, Antoine Delignat-Lavaud, Christoph Egger, Cédric Fournet, Konrad Kohbrok, and Markulf Kohlweiss. Key-schedule security for the TLS 1.3 standard. Cryptology ePrint Archive, Paper 2021/467, 2022. ASIACRYPT '22.

[BDLF+18] Chris Brzuska, Antoine Delignat-Lavaud, Cédric Fournet, Konrad Kohbrok, and Markulf Kohlweiss. State separation for code-based game-playing proofs. Cryptology ePrint Archive, Paper 2018/306, 2018. ASIACRYPT '18.

[BDPR98] Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. Relations among notions of security for public-key encryption schemes. In *CRYPTO '98*, pages 26–45, 1998.

[Bel98] Mihir Bellare. Practice-oriented provable-security. In *Lectures on Data Security*, LNCS 1561, pages 1–15. Springer, 1998.

[BF03] Dan Boneh and Matthew Franklin. Identity-based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003. Preliminary version in CRYPTO '01.

[BGB09] Gilles Barthe, Benjamin Grégoire, and Santiago Zanella Béguelin. Formal certification of code-based cryptographic proofs. In *POPL '09*, pages 90–101, 2009.

[BGHB11] Gilles Barthe, Benjamin Grégoire, Sylvain Heraud, and Santiago Zanella Béguelin. Computer-aided security proofs for the working cryptographer. In *CRYPTO '11*, pages 71–90, 2011.

[BHK09] Mihir Bellare, Dennis Hofheinz, and Eike Kiltz. Subtleties in the definition of IND-CCA: When and how should challenge-decryption be disallowed? Cryptology ePrint Archive, Paper 2009/418, 2009. J. Cryptology '15.

[BHK13] Mihir Bellare, Viet Tung Hoang, and Sriram Keelveedhi. Instantiating random oracles via UCEs. Cryptology ePrint Archive, Paper 2013/424, 2013. CRYPTO '13.

[BHR12] Mihir Bellare, Viet Tung Hoang, and Phillip Rogaway. Foundations of garbled circuits. Cryptology ePrint Archive, Paper 2012/265, 2012. ACM CCS '12.

[BJLS16] Christoph Bader, Tibor Jager, Yong Li, and Sven Schäge. On the impossibility of tight cryptographic reductions. Cryptology ePrint Archive, Paper 2015/374, 2016. EUROCRYPT '16.

[BKR94] Mihir Bellare, Joe Kilian, and Phillip Rogaway. The security of cipher block chaining. In *CRYPTO '94*, pages 341–358, 1994. Journal version in JCSS '00.

[BL13] Daniel J. Bernstein and Tanja Lange. Non-uniform cracks in the concrete: The power of free precomputation. In *ASIACRYPT '13*, pages 321–340, 2013.

[Bla06] Bruno Blanchet. A computationally sound mechanized prover for security protocols. In *IEEE S&P '06*, pages 140–154, 2006.

[BLS17] David A. Basin, Andreas Lochbihler, and S. Reza Sefidgar. CryptHOL: Game-based proofs in higher-order logic. Cryptology ePrint Archive, Paper 2017/753, 2017. J. Cryptology '20.

[BM84] Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudorandom bits. *SIAM Journal on Computing*, 13(4):850–864, 1984. Preliminary version in FOCS '82.

[BMW03] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In *EUROCRYPT '03*, pages 614–629, 2003.

[BN00] Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. Cryptology ePrint Archive, Paper 2000/025, 2000. ASIACRYPT '00.

[BN06] Mihir Bellare and Gregory Neven. Multi-signatures in the plain public-key model and a general forking lemma. In *ACM CCS '06*, pages 390–399, 2006.

[BNPS03] Mihir Bellare, Chanathip Namprempre, David Pointcheval, and Michael Semanko. The one-more-RSA-inversion problems and the security of Chaum's blind signature scheme. *Journal of Cryptology*, 16(3):185–215, 2003.

[BPR00] Mihir Bellare, David Pointcheval, and Phillip Rogaway. Authenticated key exchange secure against dictionary attacks. In *EUROCRYPT '00*, pages 139–155, 2000.

[BR93a] Mihir Bellare and Phillip Rogaway. Entity authentication and key distribution. In *CRYPTO '93*, pages 232–249, 1993.

[BR93b] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *ACM CCS '93*, pages 62–73, 1993.

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

[BR96] Mihir Bellare and Phillip Rogaway. The exact security of digital signatures — how to sign with RSA and Rabin. In *EUROCRYPT '96*, pages 399–416, 1996.

[BR04] Mihir Bellare and Phillip Rogaway. Code-based game-playing proofs and the security of triple encryption. Cryptology ePrint Archive, Paper 2004/331, 2004.

[BR06] Mihir Bellare and Phillip Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In *EUROCRYPT '06*, pages 409–426, 2006.

[BRT12] Mihir Bellare, Thomas Ristenpart, and Stefano Tessaro. Multi-instance security and its application to password-based cryptography. Cryptology ePrint Archive, Paper 2012/196, 2012. CRYPTO '12.

[BSZ05] Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of group signatures: The case of dynamic groups. In *CT-RSA '05*, pages 136–153, 2005.

[BT16] Mihir Bellare and Bjoern Tackmann. The multi-user security of authenticated encryption: AES-GCM in TLS 1.3. Cryptology ePrint Archive, Paper 2016/564, 2016. CRYPTO '16.

[Can01] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *FOCS '01*, pages 136–145, 2001. Cryptology ePrint Archive, Paper 2000/067.

[CGH04] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. *Journal of the ACM*, 51(4):557–594, 2004. Preliminary version in STOC '98.

[CK01] Ran Canetti and Hugo Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. Cryptology ePrint Archive, Paper 2001/040, 2001. EUROCRYPT '01.

[Cor00] Jean-Sébastien Coron. On the exact security of full domain hash. In *CRYPTO '00*, pages 229–235, 2000.

[CS98] Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *CRYPTO '98*, pages 13–25, 1998.

[CS03] Ronald Cramer and Victor Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. Cryptology ePrint Archive, Paper 2001/108, 2003. SIAM J. Comput. '03.

[CSV19] Ran Canetti, Alley Stoughton, and Mayank Varia. EasyUC: Using EasyCrypt to mechanize proofs of universally composable security. Cryptology ePrint Archive, Paper 2019/582, 2019. CSF '19.

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography. In *STOC '91*, pages 542–552, 1991. Journal version in SIAM J. Comput. '00.

[DEF+19] Manu Drijvers, Kasra Edalatnejad, Bryan Ford, Eike Kiltz, Julian Loss, Gregory Neven, and Igors Stepanovs. On the security of two-round multi-signatures. Cryptology ePrint Archive, Paper 2018/417, 2019. IEEE S&P '19.

[Den06] Alexander W. Dent. Fundamental problems in provable security and cryptography. Cryptology ePrint Archive, Paper 2006/278, 2006. Phil. Trans. R. Soc. A '06.

[DFGS21] Benjamin Dowling, Marc Fischlin, Felix Günther, and Douglas Stebila. A cryptographic analysis of the TLS 1.3 handshake protocol. Cryptology ePrint Archive, Paper 2020/1044, 2021. J. Cryptology '21.

[FG14] Marc Fischlin and Felix Günther. Multi-stage key exchange and the case of Google's QUIC protocol. In *ACM CCS '14*, pages 1193–1204, 2014.

[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. Preliminary version in CRYPTO '01.

[GGM84] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. In *FOCS '84*, pages 464–479, 1984. Journal version in JACM '86.

[GM82] Shafi Goldwasser and Silvio Micali. Probabilistic encryption & how to play mental poker keeping secret all partial information. In *STOC '82*, pages 365–377, 1982.

[GM84] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.

[GMR88] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2):281–308, 1988. Preliminary version: *A "Paradoxical" Solution to the Signature Problem*, FOCS '84.

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989. Preliminary version in STOC '85.

[Hal05] Shai Halevi. A plausible approach to computer-aided cryptographic proofs. Cryptology ePrint Archive, Paper 2005/181, 2005.

[HHK17] Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. A modular analysis of the Fujisaki-Okamoto transformation. Cryptology ePrint Archive, Paper 2017/604, 2017. TCC '17.

[HRM+21] Philipp G. Haselwarter, Exequiel Rivas, Antoine Van Muylder, Théo Winterhalter, Carmine Abate, Nikolaj Sidorenco, Cătălin Hriţcu, Kenji Maillard, and Bas Spitters. SSProve: A foundational framework for modular cryptographic proofs in Coq. Cryptology ePrint Archive, Paper 2021/397, 2021. CSF '21.

[JKSS12] Tibor Jager, Florian Kohlar, Sven Schäge, and Jörg Schwenk. On the security of TLS-DHE in the standard model. Cryptology ePrint Archive, Paper 2011/219, 2012. CRYPTO '12.

[KM04] Neal Koblitz and Alfred Menezes. Another look at "provable security". Cryptology ePrint Archive, Paper 2004/152, 2004. J. Cryptology '07.

[KPW13] Hugo Krawczyk, Kenneth G. Paterson, and Hoeteck Wee. On the security of the TLS protocol: A systematic analysis. Cryptology ePrint Archive, Paper 2013/339, 2013. CRYPTO '13.

[KR96] Joe Kilian and Phillip Rogaway. How to protect DES against exhaustive key search. In *CRYPTO '96*, pages 252–267, 1996.

[Lin16] Yehuda Lindell. How to simulate it — a tutorial on the simulation proof technique. Cryptology ePrint Archive, Paper 2016/046, 2016.

[LR88] Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 17(2):373–386, 1988.

[Mau02] Ueli Maurer. Indistinguishability of random systems. In *EUROCRYPT '02*, pages 110–132, 2002.

[MPR07] Ueli Maurer, Krzysztof Pietrzak, and Renato Renner. Indistinguishability amplification. In *CRYPTO '07*, pages 130–149, 2007.

[MRH04] Ueli Maurer, Renato Renner, and Clemens Holenstein. Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In *TCC '04*, pages 21–39, 2004.

[NRS21] Jonas Nick, Tim Ruffing, and Yannick Seurin. MuSig2: Simple two-round Schnorr multi-signatures. Cryptology ePrint Archive, Paper 2020/1261, 2021. CRYPTO '21.

[NY90] Moni Naor and Moti Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *STOC '90*, pages 427–437, 1990.

[PM15] Adam Petcher and Greg Morrisett. The foundational cryptography framework. In *POST '15*, pages 53–72, 2015.

[PS96] David Pointcheval and Jacques Stern. Security proofs for signature schemes. In *EUROCRYPT '96*, pages 387–398, 1996.

[Rog02] Phillip Rogaway. Authenticated-encryption with associated-data. In *ACM CCS '02*, pages 98–107, 2002.

[Rog04] Phillip Rogaway. Nonce-based symmetric encryption. In *FSE '04*, pages 348–358, 2004.

[Rog06] Phillip Rogaway. Formalizing human ignorance: Collision-resistant hashing without the keys. Cryptology ePrint Archive, Paper 2006/281, 2006. VIETCRYPT '06.

[RS91] Charles Rackoff and Daniel R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *CRYPTO '91*, pages 433–444, 1991.

[RS04] Phillip Rogaway and Thomas Shrimpton. Cryptographic hash-function basics: Definitions, implications and separations for preimage resistance, second-preimage resistance, and collision resistance. Cryptology ePrint Archive, Paper 2004/035, 2004. FSE '04.

[RS06] Phillip Rogaway and Thomas Shrimpton. A provable-security treatment of the key-wrap problem. In *EUROCRYPT '06*, pages 373–390, 2006.

[RSS11] Thomas Ristenpart, Hovav Shacham, and Thomas Shrimpton. Careful with composition: Limitations of indifferentiability and universal composability. Cryptology ePrint Archive, Paper 2011/339, 2011. EUROCRYPT '11.

[Sho97] Victor Shoup. Lower bounds for discrete logarithms and related problems. In *EUROCRYPT '97*, pages 256–266, 1997.

[Sho01] Victor Shoup. OAEP reconsidered. Cryptology ePrint Archive, Paper 2000/060, 2001. CRYPTO '01.

[Sho04] Victor Shoup. Sequences of games: A tool for taming complexity in security proofs. Cryptology ePrint Archive, Paper 2004/332, 2004.

[Yao82] Andrew C. Yao. Theory and application of trapdoor functions. In *FOCS '82*, pages 80–91, 1982.