




























<p>LaTeX Error: ! Too many }'s</p> <p>[INSERT FOOTNOTE]</p> <p> Appendix A</p>	<p>12345.</p> <p> Appendix A</p>	<p>A hardcoded hardcore bit.</p> <p> Appendix A</p>
<p>A magic black-box encryption scheme.</p> <p> Appendix A</p>	<p>A Random Oracle.</p> <p> Appendix A</p>	<p>A really contrived motivation for a really obscure primitive.</p> <p> Appendix A</p>
<p>A shy PhD student.</p> <p> Appendix A</p>	<p>A somewhat quantum-secure symmetric encryption scheme.</p> <p> Appendix A</p>	<p>A nice quiet night of sleep.</p> <p> Appendix A</p>







Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Adversary \mathcal{A}.</p> <p> Appendix A</p>	<p>Abstract.</p> <p> Appendix A</p>	<p>Alice.</p> <p> Appendix A</p>
<p>An efficient FHE Scheme.</p> <p> Appendix A</p>	<p>An exponential amount of slaves PhD students.</p> <p> Appendix A</p>	<p>An honest but lazy party.</p> <p> Appendix A</p>
<p>An uncountable amount of patience.</p> <p> Appendix A</p>	<p>Assuming “P=NP” to save your result.</p> <p> Appendix A</p>	<p>Batman.</p> <p> Appendix A</p>











Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Being closer to Kevin Bacon than Paul Erdős.</p> <p> Appendix A</p>	<p>Being GDPR compliant¹.</p> <p><i>¹This card does not store personal information.</i></p> <p> Appendix A</p>	<p>Block-Cipher.</p> <p> Appendix A</p>
<p>Bob.</p> <p> Appendix A</p>	<p>Cards Against Cryptography Solitaire.</p> <p><i>The cipher not the game.</i></p> <p> Appendix A</p>	<p>C-FAIL.</p> <p><i>Conference for Failed Approaches and Insightful Losses</i></p> <p> Appendix A</p>
<p>██████████ .</p> <p>This card has been sanitized by your local ██████ agent.</p> <p> Appendix A</p>	<p>Censoring ██████ after ██████ has told you to do so.</p> <p>██████████ is innocent!</p> <p> Appendix A</p>	<p>Chicken Chicken Chicken: Chicken Chicken.</p> <p><i>Chickens</i></p> <p> Appendix A</p>










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Circular security.</p> <p> Appendix A</p>	<p>Coming up with a scheme to match the cool acronym.</p> <p> Appendix A</p>	<p>Concerned reader.</p> <p> Appendix A</p>
<p>Confuse the reader with quantum multi-key FHE.</p> <p> Appendix A</p>	<p>Constructing a correct simulator.</p> <p> Appendix A</p>	<p>Cracking the Enigma.</p> <p> Appendix A</p>
<p>Crypto.</p> <p><i>#means#cryptography</i></p> <p> Appendix A</p>	<p>CRYPTO.</p> <p> Appendix A</p>	<p>Cryptography.</p> <p> Appendix A</p>










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Cryptomania.</p> <p> Appendix A</p>	<p>Designing an ideal functionality for scratching your nose.</p> <p> Appendix A</p>	<p>Discrete Logarithm Problem.</p> <p> Appendix A</p>
<p>Dreaming of a long Coq proof.</p> <p> Appendix A</p>	<p></p> <p><i>On Mars all birds are blue cows.</i></p> <p> Appendix A</p>	<p>Efficiency.</p> <p> Appendix A</p>
<p>Encryption scheme.</p> <p> Appendix A</p>	<p>ePrint.</p> <p> Appendix A</p>	<p>EUROCRYPT.</p> <p> Appendix A</p>










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Exercise.</p> <p> Appendix A</p>	<p>Factoring.</p> <p> Appendix A</p>	<p>Failing the Turing test.</p> <p><i>Solve the CAPTCHA to proceed.</i></p> <p> Appendix A</p>
<p>Failure.</p> <p> Appendix A</p>	<p>God.</p> <p> Appendix A</p>	<p>Having your scheme broken live during the presentation by a question from the audience.</p> <p> Appendix A</p>
<p>Hash Function.</p> <p> Appendix A</p>	<p>Hot topic.</p> <p> Appendix A</p>	<p>It's not an error, it's a typo.</p> <p> Appendix A</p>










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Introducing non-binary search.</p> <p> Appendix A</p>	<p>Kids.</p> <p> Appendix A</p>	<p>MAC.</p> <p> Appendix A</p>
<p>Multi-linear-maps.</p> <p> Appendix A</p>	<p>My favorite reviewer.</p> <p> Appendix A</p>	<p>My grandma, revisited.</p> <p> Appendix A</p>
<p>My isogeny.</p> <p> Appendix A</p>	<p>Not knowing your advisor by sight.</p> <p> Appendix A</p>	<p>LWE.</p> <p> Appendix A</p>










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Obfustopia.</p> <p> Appendix A</p>	<p>Paradise for cryptographers.</p> <p> Appendix A</p>	<p>People misspelling your name on slides.</p> <p> Appendix A</p>
<p>PRESENT, the lightweight block cipher.</p> <p> Appendix A</p>	<p>Proof by obfuscation.</p> <p> Appendix A</p>	<p>Proof by UC.</p> <p> Appendix A</p>
<p>Proof of Ignorance.</p> <p> Appendix A</p>	<p>Punctured proofs.</p> <p> Appendix A</p>	<p>Reviewers 1 & 2, but not 3.</p> <p> Appendix A</p>










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Revisited.</p> <p> Appendix A</p>	<p>Santa.</p> <p> Appendix A</p>	<p>Saving the environment by re-using your one-time pads.</p> <p> Appendix A</p>
<p>Secure.</p> <p> Appendix A</p>	<p>Secure against horde of monkeys with typewriters.</p> <p> Appendix A</p>	<p>Security.</p> <p> Appendix A</p>
<p>Seeing your work of the past 2 years uploaded to ePrint by someone else.</p> <p> Appendix A</p>	<p>Shopping.</p> <p> Appendix A</p>	<p>Shopping on AliExpress.</p> <p> Appendix A</p>










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Solving yet another problem using MPC.</p> <p> Appendix A</p>	<p>Signature Scheme.</p> <p> Appendix A</p>	<p>SIS.</p> <p> Appendix A</p>
<p>Slapping obfuscation on top of your broken construction to make it work.</p> <p> Appendix A</p>	<p>SNARK.</p> <p> Appendix A</p>	<p>Spiderpig.</p> <p> Appendix A</p>
<p>Storing my rainbow table in the cloud.</p> <p> Appendix A</p>	<p>The damn full version.</p> <p> Appendix A</p>	<p>The leftover hash lemma.</p> <p> Appendix A</p>



















Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>The Holy Grail.</p> <p>  Appendix A </p>	<p>The NSA!!!!</p> <p>  Appendix A </p>	<p>The One Ring.</p> <p>  Appendix A </p>
<p>The UC framework.</p> <p>  Appendix A </p>	<p>Those lousy students.</p> <p>  Appendix A </p>	<p>UC-secure MPC over \mathbb{Z}_q for PQS OT based on RLWE.</p> <p>  Appendix A </p>
<p>Using secure distributed deep learning to formally verify a lattice-based machine generated argument of simulated knowledge in the post-quantum universal composability framework given a random oracle.</p> <p>  Appendix A </p>	<p>Women in Computer Science.</p> <p>  Appendix A </p>	<p>Word document templates at security conferences.</p> <p>  Appendix A </p>

















Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Wonder Woman.</p> <p> Appendix A</p>	<p>Ignoring the 6000 character rebuttal.</p> <p> Appendix A</p>	<p>Your personal scribe.</p> <p> Appendix A</p>
<p>Your secretary.</p> <p> Appendix A</p>	<p>Zero Knowledge Reviewer.</p> <p> Appendix A</p>	<p>\$</p> <p> Appendix ₿</p>
<p>A buzzword which marketing came up with.</p> <p> Appendix ₿</p>	<p>Blockchain.</p> <p> Appendix ₿⁰</p>	<p>Blockchain.</p> <p> Appendix ₿¹</p>

Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Blockchain.</p> <p> Appendix </p>	<p>Blockchain.</p> <p> Appendix </p>	<p>Blockchain.</p> <p> Appendix </p>
<p>Blockchain?</p> <p> Appendix </p>	<p>Blockchains.</p> <p> Appendix </p>	<p>Blockchain, Blockchain, Blockchain.</p> <p> Appendix </p>
<p>Blockchain Engineer.</p> <p> Appendix </p>	<p>Cryptomoneya.</p> <p> Appendix </p>	<p>Hiding behind the blockchain.</p> <p> Appendix </p>

Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Mining Bitcoin.</p> <p> Appendix </p>	<p>Post blockchain cryptography</p> <p><i>also known as MPC</i></p> <p> Appendix </p>	<p>Proof-of-stake.</p> <p> Appendix </p>
<p>Proof-of-work.</p> <p> Appendix </p>	<p>Using blockchain to build a tiny house.</p> <p> Appendix </p>	<p>Using proof-of-stake to save the climate.</p> <p> Appendix </p>
<p>Using proof-of-work to heat your flat.</p> <p> Appendix </p>	<p></p>	<p></p>

Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography