Boudot's Range-Bounded Commitment Scheme Revisited

Zhengjun Cao[1] and Lihua Liu[2]

[1] Department of Mathematics, Shanghai University, Shanghai, China
caozhj@shu.edu.cn
[2] Department of Information and Computation Sciences, Shanghai Maritime University, Shanghai, China

Abstract. Checking whether a committed integer lies in a specific interval has many cryptographic applications. In Eurocrypt'98, Chan et al. proposed an instantiation (CFT Proof). Based on CFT, Boudot presented a popular range-bounded commitment scheme in Eurocrypt'2000. Both CFT Proof and Boudot Proof are based on the encryption $E(x, r) = g^x h^r \bmod n$, where n is an RSA modulus whose factorization is *unknown* by the prover. They did not use a single base as usual. Thus an increase in cost occurs. In this paper, we show that it suffices to adopt a single base. The cost of the modified Boudot Proof is about half of that of the original scheme. Moreover, the key restriction in the original scheme, i.e., both the discrete logarithm of g in base h and the discrete logarithm of h in base g are unknown by the prover, which is a potential menace to the Boudot Proof, is definitely removed.

Keywords: range-bounded commitment, knowledge of a discrete logarithm, zero-knowledge proof.

1 Introduction

Checking whether a committed integer lies in a specific interval was first developed by Brickell, et al. [2] in Crypto'87. Such kind of proofs have many applications: electronic cash systems [6], group signatures [8], publicly verifiable secret sharing schemes [16,14,4], and other zero-knowledge protocols [9]. Informally, a range-bounded commitment is a protocol between a prover, Alice, and a verifier, Bob, with which Alice commits to a string, x, and proves to Bob that x is within a predetermined range, H, with accuracy δ.

In the past decade, there are a few schemes investigating range-bounded commitments. Mao [16] proposed a scheme for proof of bit-length based on DLP (discrete logarithm problem) in PKC'98. In Eurocrypt'98, Chan et al. [6] presented an instantiation (CFT proof for short). It's corrected soon [7] because the authors did not notice that Alice can cheat Bob if the *order* of the cryptographic group is known by her. Based on CFT proof, Boudot [3] constructed a popular range-bounded commitment scheme in Eurocrypt'2000 (Boudot proof for short). The basic idea of the scheme is to decompose a committed number x as $x = x_1^2 + x_2$. It then uses Fujisaki-Okamoto commitment scheme [13] to

S. Qing, H. Imai, and G. Wang (Eds.): ICICS 2007, LNCS 4861, pp. 230–238, 2007.

show that the committed number x_1^2 is a square. By CFT proof, it proves the committed number x_2 in a proper range.

Both CFT proof and Boudot proof are based on the encryption

$$E(x, r) = g^x h^r \mod n$$

where x is the committed number, r is a random number selected by Alice, n is an RSA modulus whose factorization is unknown to Alice, g is an element of large order in $\mathbb{Z}_n$ and h is an element of the group generated by g such that both the discrete logarithm of g in base h and the discrete logarithm of h in base g are unknown by Alice. We notice that they do not use a single base as usual. Thus an increase in cost occurs.

Why not use a single base instead two bases? The reason, we think, is that they directly followed the structures of Fujisaki-Okamoto commitment [13]. In 2002, the authors [11] explained that a commitment with a single base to s of form $c = g^s \mod n$ does not satisfy the standard hiding property for commitments. For instance, if a prover commits twice to the same value, this is immediately visible. But we notice that they did not consider to permit Alice to update the single base g. Actually, if Alice commits twice to the same value, she can pick a random number θ and update the base g with $\hat{g} = g^\theta \mod n$. Note that g is still permitted to be a system-wide parameter since Alice can update it by herself. But in Fujisaki-Okamoto commitment scheme (with two bases), Alice is not permitted to update the bases. Otherwise, the discrete logarithm of $\hat{g}$ in base $\hat{h}$ or the discrete logarithm of $\hat{h}$ in base $\hat{g}$ will be known to Alice.

In this paper, we show that it suffices to adopt a single base, i.e., $E(x) = g^x \mod n$. The common encryption sufficiently guarantees the security of the modified Boudot commitment scheme. Thus the cost of the modified Boudot proof is about half of that of the original scheme. Its security is immediately reduced to RSA [18] and a variant of Schnorr signature [19] in RSA setting with hidden order. Moreover, the key restriction in the original scheme, both the discrete logarithm of g in base h and the discrete logarithm of h in base g are unknown by the prover, which is a potential menace to the Boudot proof, is definitely removed.

2 Related Work

2.1 CFT Proof

The following description of CFT proof is due to [3].

Let t, l and s be three security parameters. This protocol (due to Chan, Frankel and Tsiounis [6], and corrected in [7], and also due to [14] in another form) proves that a committed number $x \in I$ belongs to J, where the expansion rate $\#J/\#I$ is equal to 2^{t+l+1}. Let n be a large composite number whose factorization is unknown by Alice and Bob, g be an element of large order in $\mathbb{Z}_n^*$ and h be an element of the group generated by g such that both the discrete logarithm of g in base h and the discrete logarithm of h in base g are unknown by Alice. Let H be a hash function which outputs $2t$-bit strings. We denote by $E = E(x, r) = g^x h^r \mod n$ a commitment to $x \in [0, b]$, where r is randomly selected over $[-2^s n + 1, 2^s n - 1]$. This commitment statistically reveals no information about x to Bob.

Protocol. $PK_{[CFT]}(x, r : E = E(x, r) \wedge x \in [-2^{t+l}b, 2^{t+l}b])$

1. Alice picks $\omega \in_R [0, 2^{t+l}b-1]$ and $\eta \in_R [-2^{t+l+s}n+1, 2^{t+l+s}n-1]$, and then computes $W = g^{\omega}h^{\eta} \bmod n$.
2. Then, she computes $C = H(W)$ and $c = C \bmod 2^t$.
3. Finally, she computes $D_1 = \omega + xc$ and $D_2 = \eta + rc$ (in $\mathbb{Z}$). If $D_1 \in [cb, 2^{t+l}b-1]$, she sends (C, D_1, D_2) to Bob, otherwise she starts again the protocol.
4. Bob checks that $D_1 \in [cb, 2^{t+l}b-1]$ and that $C = H(g^{D_1}h^{D_2}E^{-c})$. This convinces Bob that $x \in [-2^{t+l}b, 2^{t+l}b]$.

2.2 Proof That Two Commitments Hide the Same Secret

Alice secretly holds $x \in [0, b]$. Let $E = E_1(x, r_1)$ and $F = E_2(x, r_2)$ be two commitments to x. She wants to prove to Bob that she knows x, r_1, r_2 such that $E = E_1(x, r_1)$ and $F = E_2(x, r_2)$, i.e. that E and F hide the same secret x. This protocol is derived from proofs of equality of two discrete logarithms from [10,5,1], combined with a proof of knowledge of a discrete logarithm modulo n [15].

Protocol. $PK(x, r_1, r_2 : E = E_1(x, r_1) \wedge F = E_2(x, r2))$

1. Alice picks $\omega \in_R [1, 2^{l+t}b-1], \eta_1 \in_R [1, 2^{l+t+s_1}n-1], \eta_2 \in_R [1, 2^{l+t+s_2}n-1]$. Then, she computes $W_1 = g_1^{\omega}h_1^{\eta_1} \bmod n$ and $W_2 = g_2^{\omega}h_2^{\eta_2} \bmod n$.
2. Alice computes $c = H(W_1||W_2)$.
3. She computes $D = \omega + cx, D_1 = \eta_1 + cr_1, D_2 = \eta_2 + cr_2$ (in $\mathbb{Z}$) and sends (c, D, D_1, D_2) to Bob.
4. Bob checks whether $c = H(g_1^D h_1^{D_1} E^{-c} \bmod n || g_2^D h_2^{D_2} F^{-c} \bmod n)$.

2.3 Proof That a Committed Number Is a Square

Alice secretly holds $x \in [0, b]$. Let $E = E(x^2, r_1)$ be a commitment to the square of x (in $\mathbb{Z}$). She wants to prove to Bob that she knows x and r_1 such that $E = E(x^2, r_1)$, i.e. that E hides the square x^2. The first proof that a committed number is a square has appeared in [13].

Protocol. $PK(x, r_1 : E = E(x^2, r_1))$

1. Alice picks $r_2 \in_R [-2^s n+1, 2^s n-1]$ and computes $F = E(x, r_2)$.
2. Then, Alice computes $r_3 = r_1 - r_2 x$ (in $\mathbb{Z}$). Note that $r_3 \in [-2^s bn+1, 2^s bn-1]$. Then, $E = F^x h^{r_3} \bmod n$.
3. As E is a commitment to x in base (F, h) and F is a commitment to x in base (g, h), Alice can run $PK(x, r_2, r_3 : F = g^x h^{r_2} \bmod n \wedge E = F^x h^{r_3} \bmod n)$. By the proof that two commitments hide the same secret described above, she gets (c, D, D_1, D_2).
4. She sends (F, c, D, D_1, D_2) to Bob.
5. Bob checks that $PK(x, r_2, r_3 : F = g^x h^{r_2} \bmod n \wedge E = F^x h^{r_3} \bmod n)$ is valid.

2.4 Boudot Proof

Let t, l and s be three security parameters. Let n be a large composite number whose factorization is unknown by Alice and Bob, g be an element of large order

in $\mathbb{Z}_n^*$ and h be an element of the group generated by g such that both the discrete logarithm of g in base h and the discrete logarithm of h in base g are unknown by Alice. We denote by $E(x,r) = g^x h^r \bmod n$ a commitment to x in base (g,h) where r is randomly selected over $[-2^s n + 1, 2^s n - 1]$.

Protocol. $PK_{[WithTol]}(x, r : E = E(x,r) \wedge x \in [a - \theta, b + \theta])$

1. [Knowledge of x] Alice executes with Bob: $PK(x, r : E = E(x,r))$
2. [Setting] Both Alice and Bob compute $\widetilde{E} = E/g^a \bmod n$ and $\bar{E} = g^b/E \bmod n$. Alice sets $\widetilde{x} = x - a$ and $\bar{x} = b - x$. Now, Alice must prove to Bob that both $\widetilde{E}$ and $\bar{E}$ hide secrets which are greater than $-\theta$.
3. [Decomposition of $\widetilde{x}$ and $\bar{x}$] Alice computes:
$$\widetilde{x}_1 = \lfloor \sqrt{x - a} \rfloor, \qquad \widetilde{x}_2 = \widetilde{x} - \widetilde{x}_1^2,$$
$$\bar{x}_1 = \lfloor \sqrt{b - x} \rfloor, \qquad \bar{x}_2 = \bar{x} - \bar{x}_1^2$$
Then, $\widetilde{x} = \widetilde{x}_1^2 + \widetilde{x}_2$and $\bar{x} = \bar{x}_1^2 + \bar{x}_2$, where $0 \leq \widetilde{x}_2 \leq 2\sqrt{b-a}$ and $0 \leq \bar{x}_2 \leq 2\sqrt{b-a}$.
4. [Choice of random values for new commitments] Alice randomly selects $\widetilde{r}_1$ and $\widetilde{r}_2$ in $[-2^s n + 1, \cdots, 2^s n - 1]$ such that $\widetilde{r}_1 + \widetilde{r}_2 = r$, and $\bar{r}_1$ and $\bar{r}_2$ such that $\bar{r}_1 + \bar{r}_2 = -r$.
5. [Computation of new commitments] Alice computes:
$$\widetilde{E}_1 = E(\widetilde{x}_1^2, \widetilde{r}_1), \qquad \widetilde{E}_2 = E(\widetilde{x}_2, \widetilde{r}_2)$$
$$\bar{E}_1 = E(\bar{x}_1^2, \bar{r}_1), \qquad \bar{E}_2 = E(\bar{x}_2, \bar{r}_2)$$
6. [Sending of the new commitments] Alice sends $\widetilde{E}_1$ and $\bar{E}_1$ to Bob. Bob computes $\widetilde{E}_2 = \widetilde{E}/\widetilde{E}_1$ and $\bar{E}_2 = \bar{E}/\bar{E}_1$
7. [Validity of the commitments to a square] Alice executes with Bob
$$PK(\widetilde{x}_1^2, \widetilde{r}_1 : \widetilde{E}_1 = E(\widetilde{x}_1^2, \widetilde{r}_1))$$
$$PK(\bar{x}_1^2, \bar{r}_1 : \bar{E}_1 = E(\bar{x}_1^2, \bar{r}_1))$$
which prove that both $\widetilde{E}_1$ and $\bar{E}_1$ hide a square.
8. [Validity of the commitments to a small value] Let $\theta = 2^{t+l+1}\sqrt{b-a}$. Alice executes with Bob the two following CFT proofs:
$$PK_{[CFT]}(\widetilde{x}_2, \widetilde{r}_2 : \widetilde{E}_2 = E(\widetilde{x}_2, \widetilde{r}_2) \wedge \widetilde{x}_2 \in [-\theta, \theta])$$
$$PK_{[CFT]}(\bar{x}_2, \bar{r}_2 : \bar{E}_2 = E(\bar{x}_2, \bar{r}_2) \wedge \bar{x}_2 \in [-\theta, \theta])$$
which prove that both $\widetilde{E}_2$ and $\bar{E}_2$ hide numbers which belong to $[-\theta, \theta]$, where $\theta = 2^{t+l+1}\sqrt{b-a}$, instead of proving that they belong to $[0, 2\sqrt{b-a}]$.

3 It Suffices to Adopt a Single Base

We remark that all above commitment schemes are based on the encryption

$$E(x,r) = g^x h^r \mod n$$

where x is the committed number, r is a random number selected by Alice, n is an RSA modulus whose factorization is *unknown* by Alice, g is an element of large order in $\mathbb{Z}_n$ and h is an element of the group generated by g such that both the discrete logarithm of g in base h and the discrete logarithm of h in base g are unknown by Alice.

We notice that they do not use a single base as usual. Thus an increase in cost occurs. In the next section, we show that it suffices to adopt a single base, i.e.,

$$E(x) = g^x \mod n$$

The common encryption sufficiently guarantees the securities of those commitment schemes. Thus the cost of the modified Boudot proof is about half of that of the original scheme. Besides, its security is immediately reduced to RSA [18] and a variant of Schnorr signature [19] in RSA setting with hidden order.

4 Modified CFT Proof and Its Security

4.1 Description

Let t, l and s be three security parameters, n be an RSA modulus whose factorization is *unknown* by Alice, g be an element of large order in $\mathbb{Z}_n^*$. Let H be a hash function which outputs $2t$-bit strings. We denote by $E = E(x) = g^x \mod n$ a commitment to $x \in [0, b]$.

Protocol. $PK(x : E = E(x) \wedge x \in [-2^{t+l}b, 2^{t+l}b])$

1. Alice picks $\omega \in_R [0, 2^{t+l}b - 1]$, and computes $W = g^\omega \mod n$.
2. Compute $C = H(W)$ and $c = C \mod 2^t$.
3. Compute $D = \omega + xc$ (in $\mathbb{Z}$). If $D \in [cb, 2^{t+l}b - 1]$, Alice sends (C, D) to Bob, otherwise she starts again the protocol.
4. Bob checks that $D \in [cb, 2^{t+l}b - 1]$ and $C = H(g^D E^{-c} \mod n)$. This convinces Bob that $x \in [-2^{t+l}b, 2^{t+l}b]$.

4.2 Security

It's not difficult to find that the modified scheme is almost as secure as the original scheme. Informally, the security of the modified scheme is just based on the following facts:

(F1) By the security of RSA [18], the single base encryption $E = E(x) = g^x \mod n$ effectively prevents Bob from getting x.

(F2) Alice knows the discrete logarithm of E in base g modulo n. Otherwise, she cannot produce a proper pair (C, D) such that $C = H(g^D E^{-c} \mod n)$, where $c = C \mod 2^t$, t is a public security parameter. Note that the above challenge is just the variant of Schnorr signature [19] in RSA setting. Under the circumstances, Alice cannot cheat Bob even she knows the order of g. We refer to [17].

(F3) D must be of the form $\alpha + xc$, where x is the just discrete logarithm of E in base g, α is selected by Alice before the challenge value C ($\equiv c \bmod 2^t$) is generated. This is immediately derived from the fact (F2).
(F4) The factorization of the modulus n is *unknown* by Alice, which implies that $\alpha + xc$ is just an integer (not a residue class). By checking $D \in [cb, 2^{t+l}b - 1]$, it ensures that Bob can be convinced that $x \in [-2^{t+l}b, 2^{t+l}b]$.

Remark 1. The authors [6] gave the original presentation of CFT proof in ElGamal setting [12]. It's corrected soon [7] because Alice can cheat Bob if the *order* of the cryptographic group is *known* by her.

5 Same-Secret Proof with Single Base

Let n be an RSA modulus whose factorization is *unknown* by Alice, g_1 and g_2 be two element of large order in $\mathbb{Z}_n^*$. Let H be a hash function which outputs $2t$-bit strings. Alice secretly holds x. Let $E = E_1(x) = g_1^x \bmod n$ and $F = E_2(x) = g_2^x \bmod n$ be two commitments to x. She wants to prove to Bob that she knows x such that $E = E_1(x)$ and $F = E_2(x)$, i.e. that E and F hide the same secret x.

Protocol. $PK(x : E = E_1(x) \wedge F = E_2(x))$

1. Alice picks $\omega \in_R \mathbb{Z}$ and computes $W_1 = g_1^\omega \bmod n$ and $W_2 = g_2^\omega \bmod n$.
2. She computes $C = H(W_1 || W_2)$.
3. She computes $D = \omega + cx$ (in $\mathbb{Z}$) and sends (C, D) to Bob.
4. Bob checks whether $C = H(g_1^D E^{-C} \bmod n || g_2^D F^{-C} \bmod n)$.

Remark 2. One might argue a proof that two commitments hide the same secret in ElGamal setting. Precisely, it only shows that two commitments hide the same secret *residue class* (modulo the *order* of the cryptographic group) instead of the same secret *integer*.

6 Square-Proof with Single Base

Let n be an RSA modulus whose factorization is *unknown* by Alice, g be an element of large order in $\mathbb{Z}_n^*$. Let H be a hash function which outputs $2t$-bit strings. Alice secretly holds x. Let $E = E(x^2) = g^{x^2}$ be a commitment to the square of x (in $\mathbb{Z}$). She wants to prove to Bob that she knows x such that $E = E(x^2)$, i.e. that E hides the square x^2.

Protocol. $PK(x : E = E(x^2))$

1. Alice computes $F = E(x), E = F^x \bmod n$.
2. As E is a commitment to x in base F and F is a commitment to x in base g, Alice can run $PK(x : F = g^x \bmod n \wedge E = F^x \bmod n)$. By the proof that two commitments hide the same secret described above, she gets (C, D).
3. She sends (F, C, D) to Bob.
4. Bob checks that $PK(x : F = g^x \bmod n \wedge E = F^x \bmod n)$ is valid.

7 Boudot's Proof Revisited

7.1 Description

Let t, l and s be three security parameters. Let n be an RSA modulus whose factorization is *unknown* by Alice and Bob, g be an element of large order in $\mathbb{Z}_n^*$. We denote by $E(x) = g^x \bmod n$ a commitment to x in base g.

Protocol. $PK_{[WithTol]}(x : E = E(x) \wedge x \in [a - \theta, b + \theta])$

1. [Knowledge of x] Alice executes with Bob: $PK(x : E = E(x))$
2. [Setting] Both Alice and Bob compute $\widetilde{E} = E/g^a \bmod n$ and $\bar{E} = g^b/E \bmod n$. Alice sets $\widetilde{x} = x - a$ and $\bar{x} = b - x$.
3. [Decomposition of $\widetilde{x}$ and $\bar{x}$] Alice computes:
$$\widetilde{x}_1 = \lfloor \sqrt{x - a} \rfloor, \qquad \widetilde{x}_2 = \widetilde{x} - \widetilde{x}_1^2,$$
$$\bar{x}_1 = \lfloor \sqrt{b - x} \rfloor, \qquad \bar{x}_2 = \bar{x} - \bar{x}_1^2$$
Then, $\widetilde{x} = \widetilde{x}_1^2 + \widetilde{x}_2$ and $\bar{x} = \bar{x}_1^2 + \bar{x}_2$, where $0 \leq \widetilde{x}_2 \leq 2\sqrt{b - a}$ and $0 \leq \bar{x}_2 \leq 2\sqrt{b - a}$.
4. [Computation of new commitments] Alice computes:
$$\widetilde{E}_1 = E(\widetilde{x}_1^2), \qquad \widetilde{E}_2 = E(\widetilde{x}_2)$$
$$\bar{E}_1 = E(\bar{x}_1^2), \qquad \bar{E}_2 = E(\bar{x}_2)$$
5. [Sending of the new commitments] Alice sends $\widetilde{E}_1$ and $\bar{E}_1$ to Bob. Bob computes $\widetilde{E}_2 = \widetilde{E}/\widetilde{E}_1$ and $\bar{E}_2 = \bar{E}/\bar{E}_1$
6. [Validity of the commitments to a square] Alice executes with Bob
$$PK(\widetilde{x}_1^2 : \widetilde{E}_1 = E(\widetilde{x}_1^2))$$
$$PK(\bar{x}_1^2 : \bar{E}_1 = E(\bar{x}_1^2))$$
which prove that both $\widetilde{E}_1$ and $\bar{E}_1$ hide a square. (Note that the protocols $PK(x : E = E_1(x) \wedge F = E_2(x))$ and $PK(x : E = E(x^2))$ are called in the step.)
7. [Validity of the commitments to a small value] Let $\theta = 2^{t+l+1}\sqrt{b - a}$. Alice executes with Bob the two following CFT proofs:
$$PK_{[CFT]}(\widetilde{x}_2 : \widetilde{E}_2 = E(\widetilde{x}_2) \wedge \widetilde{x}_2 \in [-\theta, \theta])$$
$$PK_{[CFT]}(\bar{x}_2 : \bar{E}_2 = E(\bar{x}_2) \wedge \bar{x}_2 \in [-\theta, \theta])$$
which prove that both $\widetilde{E}_2$ and $\bar{E}_2$ hide numbers which belong to $[-\theta, \theta]$, where $\theta = 2^{t+l+1}\sqrt{b - a}$.

The correctness arguments for the modified Boudot proof are the same as that of the original scheme. We refer to [3]. But its security is immediately reduced to RSA and a variant of Schnorr signature in RSA setting with hidden order. We refer to §4.2. We remark that the reason of adopting two bases instead of a single base in Boudot proof is that the protocol directly follows the structures of [13].

7.2 Further Discussion

1. Why not use a single base instead two bases. In 2002, the authors [11] explained that:

> A commitment with a single base to s of form $c = g^s \bmod n$ does not satisfy the standard hiding property for commitments. For instance, if a prover commits twice to the same value, this is immediately visible.

Obviously, they did not consider to permit the prover to update the single base.

Now we suggest a solution to this problem. If Alice commits twice to the same value, she can pick a random θ and update the base g with $\hat{g} = g^{\theta} \bmod n$. Note that g is still permitted to be a system-wide parameter since Alice can update it by herself. But in Fujisaki-Okamoto commitment scheme (with two bases), Alice is not permitted to update the bases. Otherwise, the discrete logarithm of $\hat{g}$ in base $\hat{h}$ or the discrete logarithm of $\hat{h}$ in base $\hat{g}$ will be known to Alice.

2. Efficiency. Roughly speaking, the cost of the commitment with a single base (excluding the cost of updating the base) is about half of that of Damgård-Fujisaki commitment [11]. But the key restriction, both the discrete logarithm of g in base h and the discrete logarithm of h in base g are unknown by Alice, which is a potential menace to Damgård-Fujisaki commitment, is definitely removed. We remark that the updating of g can be completed in the pre-computation.

8 Conclusion

In this paper, we investigate the two range-bounded commitment schemes, i.e., CFT proof and Boudot proof. Based on the latter, we present an efficient range-bounded commitment. The cost of the modified scheme is about half of that of the original scheme because we adopt a single base instead of two bases. Moreover, its security is immediately reduced to RSA and a variant of Schnorr signature in RSA setting with hidden order.

References

1. Bao, F.: An Efficient Verifiable Encryption Scheme for Encryption of Discrete Logarithms. In: Schneier, B., Quisquater, J.-J. (eds.) CARDIS 1998. LNCS, vol. 1820, Springer, Heidelberg (2000)
2. Brickell, E., Chaum, D., Damgård, I., Van de Graaf, J.: Gradual and Verifiable Release of a Secret. In: Pomerance, C. (ed.) CRYPTO 1987. LNCS, vol. 293, pp. 156–166. Springer, Heidelberg (1988)
3. Boudot, F.: Efficient Proofs that a Committed Number Lies in an Interval. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 431–444. Springer, Heidelberg (2000)
4. Boudot, F., Traoré, J.: Efficient Publicly Verifiable Secret Sharing Schemes with Fast or Delayed Recovery. In: Varadharajan, V., Mu, Y. (eds.) ICICS 1999. LNCS, vol. 1726, pp. 87–102. Springer, Heidelberg (1999)

5. Chaum, D., Evertse, J.-H., Van de Graaf, J.: An Improved Protocol for Demonstrating Possession of Discrete Logarithm and Some Generalizations. In: Price, W.L., Chaum, D. (eds.) EUROCRYPT 1987. LNCS, vol. 304, pp. 127–141. Springer, Heidelberg (1988)
6. Chan, A., Frankel, Y., Tsiounis, Y.: Easy Come Easy Go Divisible Cash. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 561–575. Springer, Heidelberg (1998)
7. Chan, A., Frankel, Y., Tsiounis, Y.: Easy Come Easy Go Divisible Cash. Updated version with corrections, GTE Tech. Rep. (1998), available at: `http://www.ccs.neu.edu/home/yiannis/`
8. Camenisch, J., Michels, M.: Separability and Efficiency for Generic Group Signature Schemes. In: Wiener, M.J. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 413–430. Springer, Heidelberg (1999)
9. Camenisch, J., Michels, M.: Proving in Zero-Knowledge that a Number is the Product of Two Safe Primes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 106–121. Springer, Heidelberg (1999)
10. Chaum, D., Pedersen, T.-P.: Wallet Databases with Observers. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 89–105. Springer, Heidelberg (1993)
11. Damgård, I., Fujisaki, E.: A Statistically-Hiding Integer Commitment Scheme Based on Groups with Hidden Order. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 125–142. Springer, Heidelberg (2002)
12. ElGamal, T.: A public-key cryptosystem and a signature scheme based on discrete logarithms. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 10–18. Springer, Heidelberg (1985)
13. Fujisaki, E., Okamoto, T.: Statistical Zero Knowledge Protocols to Prove Modular Polynomial Relations. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 16–30. Springer, Heidelberg (1997)
14. Fujisaki, E., Okamoto, T.: A Practical and Provably Secure Scheme for Publicly Verifiable Secret Sharing and Its Applications. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 32–46. Springer, Heidelberg (1998)
15. Girault, M.: Self-Certified Public Keys. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 490–497. Springer, Heidelberg (1991)
16. Mao, W.: Guaranteed Correct Sharing of Integer Factorization with Off-line Shareholders. Proceedings of Public Key Cryptography 98, 27–42 (1998)
17. Pointcheval, D., Stern, J.: Security proofs for signature schemes. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 387–398. Springer, Heidelberg (1996)
18. Rivest, R., Shamir, A., Adleman, L.M.: A Mehtod for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of ACM 21(2), 120–126 (1978)
19. Schnorr, C.-P.: Efficient Signature Generation for Smart Cards. Journal of Cryptology, 239–252 (1991)